

# *P-2602H WLNI Series*

*802.11g Wireless ADSL2+ 4-Port VoIP IAD*

## **User's Guide**

Version 3.40  
9/2007  
Edition 2

### **DEFAULT LOGIN**

<b>IP Address</b>	<b>http://192.168.1.1</b>
<b>Administrator Name</b>	<b>admin</b>
<b>Administrator Password</b>	<b>admin</b>
<b>User Name</b>	<b>user</b>
<b>User Password</b>	<b>1234</b>

---

**ZyXEL**  
[www.zyxel.com](http://www.zyxel.com)



# About This User's Guide

## Intended Audience

This manual is intended for people who want to configure the ZyXEL Device using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

## Related Documentation

- Quick Start Guide  
The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.
- Web Configurator Online Help  
Embedded web help for descriptions of individual screens and supplementary information.



---

It is recommended you use the web configurator to configure the ZyXEL Device.

---

- Supporting Disk  
Refer to the included CD for support documents.
- ZyXEL Web Site  
Please refer to [www.zyxel.com](http://www.zyxel.com) for additional support documentation and product certifications.

## User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,  
ZyXEL Communications Corp.,  
6 Innovation Road II,  
Science-Based Industrial Park,  
Hsinchu, 300, Taiwan.

E-mail: [techwriters@zyxel.com.tw](mailto:techwriters@zyxel.com.tw)

# Document Conventions

## Warnings and Notes

These are how warnings and notes are shown in this User's Guide.



---

**Warnings tell you about things that could harm you or your device.**

---



---

**Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.**

---

## Syntax Conventions

- The P-2602HWLNI may be referred to as the “ZyXEL Device”, the “device”, the “system” or the “product” in this User’s Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the “enter” or “return” key on your keyboard.
- “Enter” means for you to type one or more characters and then press the [ENTER] key. “Select” or “choose” means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the “metric” value or the “scientific” value. For example, “k” for kilo may denote “1000” or “1024”, “M” for mega may denote “1000000” or “1048576” and so on.
- “e.g.,” is a shorthand for “for instance”, and “i.e.,” means “that is” or “in other words”.

## Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The ZyXEL Device icon is not an exact representation of your device.

ZyXEL Device 	Computer 	Notebook computer 
Server 	DSLAM 	Firewall 
Telephone 	Switch 	Router 

# Safety Warnings

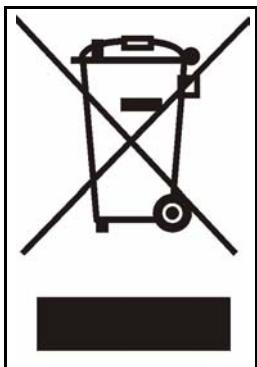


For your safety, be sure to read and follow all warning notices and instructions.

---

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).

This product is recyclable. Dispose of it properly.





# Contents Overview

<b>Introduction .....</b>	<b>39</b>
Introducing the ZyXEL Device .....	41
Introducing the Web Configurator .....	49
<b>Wizards and Status .....</b>	<b>61</b>
Internet and Wireless Setup Wizard .....	63
VoIP Wizard .....	77
Bandwidth Management Wizard .....	83
Status Screens .....	87
<b>Network .....</b>	<b>99</b>
WAN Setup .....	101
LAN Setup .....	117
Wireless LAN .....	129
Network Address Translation (NAT) Screens .....	155
<b>VoIP .....</b>	<b>167</b>
Voice .....	169
VoIP Trunking .....	211
Phone Usage .....	227
<b>Security .....</b>	<b>231</b>
Firewalls .....	233
Firewall Configuration .....	245
Content Filtering .....	265
Introduction to IPSec .....	269
VPN Screens .....	275
Certificates .....	301
<b>Advanced .....</b>	<b>325</b>
Static Route .....	327
Bandwidth Management .....	331
Dynamic DNS Setup .....	339
Remote Management Configuration .....	343
Universal Plug-and-Play (UPnP) .....	361

<b>Maintenance and Troubleshooting .....</b>	<b>373</b>
System .....	375
Call History .....	381
Logs .....	387
Troubleshooting .....	401
Tools .....	407
Diagnostic .....	419
Product Specifications .....	423
<b>Appendices and Index .....</b>	<b>433</b>

# Table of Contents

<b>About This User's Guide .....</b>	<b>3</b>
<b>Document Conventions.....</b>	<b>4</b>
<b>Safety Warnings.....</b>	<b>6</b>
<b>Contents Overview .....</b>	<b>9</b>
<b>Table of Contents.....</b>	<b>11</b>
<b>List of Figures .....</b>	<b>25</b>
<b>List of Tables.....</b>	<b>33</b>
<b>Part I: Introduction.....</b>	<b>39</b>
<b>Chapter 1</b>	
<b>Introducing the ZyXEL Device .....</b>	<b>41</b>
1.1 Overview .....	41
1.2 Ways to Manage the ZyXEL Device .....	42
1.3 Good Habits for Managing the ZyXEL Device .....	42
1.4 Applications for the ZyXEL Device .....	43
1.4.1 Internet Access .....	43
1.4.2 Making Calls via Internet Telephony Service Provider .....	43
1.4.3 Make Peer-to-peer Calls .....	44
1.4.4 Firewall for Secure Broadband Internet Access .....	44
1.4.5 LAN to LAN Application .....	45
1.5 LEDs .....	46
1.6 The RESET Button .....	47
1.6.1 Using The Reset Button .....	47
<b>Chapter 2</b>	
<b>Introducing the Web Configurator .....</b>	<b>49</b>
2.1 Web Configurator Overview .....	49
2.1.1 Accessing the Web Configurator .....	49
2.2 Login Types .....	50
2.2.1 User Access .....	50
2.2.2 Administrator Access .....	50
2.3 Web Configurator Main Screen .....	52

## Table of Contents

---

2.3.1 Title Bar .....	53
2.3.2 Navigation Panel .....	53
2.3.3 Main Window .....	59
2.3.4 Status Bar .....	59
<b>Part II: Wizards and Status.....</b>	<b>61</b>
<b>Chapter 3</b>	
<b>Internet and Wireless Setup Wizard.....</b>	<b>63</b>
3.1 Introduction .....	63
3.2 Internet Access Wizard Setup .....	63
3.2.1 Manual Configuration .....	66
3.3 Wireless Connection Wizard Setup .....	71
3.3.1 Manually Assign a WPA-PSK Key .....	74
3.3.2 Manually Assign a WEP Key .....	74
<b>Chapter 4</b>	
<b>VoIP Wizard .....</b>	<b>77</b>
4.1 Introduction .....	77
4.2 VoIP Wizard Setup .....	77
<b>Chapter 5</b>	
<b>Bandwidth Management Wizard.....</b>	<b>83</b>
5.1 Introduction .....	83
5.2 Bandwidth Management Wizard Setup .....	83
<b>Chapter 6</b>	
<b>Status Screens .....</b>	<b>87</b>
6.1 Status Screen .....	87
6.2 Any IP Table .....	91
6.3 WLAN Status .....	92
6.4 Packet Statistics .....	92
6.5 VoIP Statistics .....	94
6.6 LED Status .....	96
<b>Part III: Network.....</b>	<b>99</b>
<b>Chapter 7</b>	
<b>WAN Setup.....</b>	<b>101</b>
7.1 WAN Overview .....	101

7.1.1 Encapsulation .....	101
7.1.2 Multiplexing .....	102
7.1.3 VPI and VCI .....	102
7.1.4 IP Address Assignment .....	102
7.1.5 Nailed-Up Connection (PPP) .....	103
7.1.6 NAT .....	103
7.2 Metric .....	103
7.3 Traffic Shaping .....	104
7.3.1 ATM Traffic Classes .....	105
7.4 Zero Configuration Internet Access .....	105
7.5 Internet Access Setup .....	106
7.5.1 Advanced Internet Access Setup .....	108
7.6 WAN More Connections .....	109
7.7 More Connections Edit .....	110
7.8 More Connections Edit Advanced .....	113
7.9 Traffic Redirect .....	114
7.10 WAN Backup Setup .....	114
<b>Chapter 8</b> <b>LAN Setup.....</b>	<b>117</b>
8.1 LAN Overview .....	117
8.1.1 LANs, WANs and the ZyXEL Device .....	117
8.1.2 DHCP Setup .....	118
8.2 DNS Server Addresses .....	118
8.3 LAN TCP/IP .....	118
8.3.1 IP Address and Subnet Mask .....	118
8.3.2 RIP Setup .....	120
8.3.3 Multicast .....	120
8.3.4 Any IP .....	121
8.4 Configuring LAN IP .....	122
8.4.1 Configuring Advanced LAN Setup .....	123
8.5 DHCP Setup .....	124
8.6 LAN Client List .....	125
8.7 LAN IP Alias .....	126
<b>Chapter 9</b> <b>Wireless LAN.....</b>	<b>129</b>
9.1 Wireless Network Overview .....	129
9.2 Wireless Security Overview .....	130
9.2.1 SSID .....	130
9.2.2 MAC Address Filter .....	130
9.2.3 User Authentication .....	130
9.2.4 Encryption .....	131

## Table of Contents

---

9.2.5 One-Touch Intelligent Security Technology (OTIST) .....	132
9.3 Wireless Performance Overview .....	132
9.3.1 Quality of Service (QoS) .....	132
9.3.2 Wireless Distribution System (WDS) .....	132
9.4 Additional Wireless Terms .....	133
9.5 General WLAN Screen .....	133
9.5.1 No Security .....	134
9.5.2 WEP Encryption Screen .....	135
9.5.3 WPA(2)-PSK .....	136
9.5.4 WPA(2) Authentication Screen .....	138
9.5.5 Wireless LAN Advanced Setup .....	139
9.6 OTIST Screen .....	140
9.6.1 Notes on OTIST .....	143
9.7 MAC Filter .....	143
9.8 Association List .....	145
9.9 QoS Screen .....	145
9.9.1 Application Priority Configuration .....	147
9.10 WDS Screen .....	148
9.10.1 Static WEP .....	149
9.10.2 WPA-PSK .....	150
9.10.3 WPA2-PSK .....	152
<b>Chapter 10</b> <b>Network Address Translation (NAT) Screens.....</b>	<b>155</b>
10.1 NAT General Overview .....	155
10.1.1 NAT Definitions .....	155
10.1.2 What NAT Does .....	156
10.1.3 How NAT Works .....	156
10.1.4 NAT Application .....	156
10.1.5 NAT Mapping Types .....	157
10.2 SUA (Single User Account) Versus NAT .....	158
10.3 NAT General Setup .....	158
10.4 Port Forwarding .....	159
10.4.1 Default Server IP Address .....	160
10.4.2 Port Forwarding: Services and Port Numbers .....	160
10.4.3 Configuring Servers Behind Port Forwarding (Example) .....	160
10.5 Configuring Port Forwarding .....	161
10.5.1 Port Forwarding Rule Edit .....	162
10.6 Address Mapping .....	163
10.6.1 Address Mapping Rule Edit .....	164
<b>Part IV: VoIP .....</b>	<b>167</b>

**Chapter 11**

<b>Voice.....</b>	<b>169</b>
11.1 Introduction to VoIP .....	169
11.2 SIP .....	169
11.2.1 SIP Identities .....	169
11.2.2 SIP Servers .....	170
11.2.3 RTP .....	173
11.2.4 Pulse Code Modulation .....	173
11.2.5 SIP Call Progression .....	173
11.2.6 SIP Call Progression Through Proxies .....	173
11.2.7 Voice Coding .....	175
11.2.8 PSTN Call Setup Signaling .....	175
11.2.9 MWI (Message Waiting Indication) .....	175
11.2.10 Custom Tones (IVR) .....	176
11.3 Quality of Service (QoS) .....	176
11.3.1 Type Of Service (ToS) .....	177
11.3.2 DiffServ .....	177
11.3.3 VLAN .....	177
11.4 SIP Settings Screen .....	178
11.5 Advanced SIP Setup Screen .....	179
11.6 SIP QoS Screen .....	182
11.7 Phone .....	183
11.7.1 PSTN Line .....	183
11.7.2 ISDN Line .....	184
11.7.3 Voice Activity Detection/Silence Suppression .....	184
11.7.4 Comfort Noise Generation .....	184
11.7.5 Echo Cancellation .....	184
11.8 Analog Phone .....	184
11.8.1 PHONE Port Call Types .....	184
11.8.2 Configuring the Analog Phone Screen .....	185
11.9 Advanced Analog Phone Setup Screen .....	187
11.10 ISDN Phone .....	189
11.10.1 ISDN Phone Port Call Types .....	189
11.10.2 Configuring the ISDN Phone Screen .....	190
11.11 Common Phone Settings Screen .....	191
11.12 Ext. Table .....	191
11.13 Advanced Ext. Table Setup Screen .....	193
11.14 Phone Services Overview .....	194
11.14.1 The Flash Key .....	195
11.14.2 Europe Type Supplementary Phone Services .....	195
11.14.3 USA Type Supplementary Services .....	196
11.15 Phone Region Screen .....	198
11.16 Speed Dial .....	198

## Table of Contents

---

11.17 Incoming Call Policy Screen .....	200
11.18 Distinctive Ring Screen .....	202
11.19 SIP Prefix Screen .....	204
11.20 PSTN Line .....	206
11.21 PSTN Line Screen .....	206
11.22 ISDN Line Screen .....	207
11.23 Fixed Line Numbers .....	208
11.23.1 Multiple Subscriber Numbers .....	208
11.23.2 Receiving Analog Calls With Digital Phones .....	209
11.23.3 Configuring the Fixed Line Numbers Screen .....	209
<b>Chapter 12</b> <b>VoIP Trunking .....</b>	<b>211</b>
12.1 VoIP Trunking Overview .....	211
12.2 VoIP Trunking and Security .....	211
12.2.1 Auto Attendant and Authentication .....	211
12.2.2 Peer Call Authentication .....	212
12.3 Call Rules .....	213
12.4 VoIP Trunking Scenarios .....	213
12.4.1 VoIP Phone To PSTN Phone .....	213
12.4.2 PSTN Phone To VoIP Phone .....	213
12.4.3 PSTN Phone To PSTN Phone via VoIP .....	214
12.5 Trunking General Screen .....	214
12.6 Trunking Peer Call Screen .....	215
12.7 Trunking Call Rule Screen .....	217
12.8 VoIP Trunking Example: VoIP to PSTN .....	219
12.8.1 Background Information .....	219
12.8.2 Configuration Details: Outgoing .....	219
12.8.3 Configuration Details: Incoming .....	220
12.8.4 Call Progression .....	221
12.9 VoIP Trunking Example: PSTN to PSTN via VoIP .....	221
12.9.1 Background Information .....	222
12.9.2 Configuration Details: Outgoing .....	222
12.9.3 Configuration Details: Incoming .....	224
12.9.4 Call Progression .....	224
<b>Chapter 13</b> <b>Phone Usage .....</b>	<b>227</b>
13.1 Dialing a Telephone Number .....	227
13.2 Using Speed Dial to Dial a Telephone Number .....	227
13.3 Internal Calls .....	227
13.3.1 Phone Book .....	228
13.3.2 Call Transfer .....	228

13.3.3 Call Forwarding .....	228
13.3.4 Follow Me .....	228
13.3.5 Call Pickup .....	229
13.4 Checking the Device's IP Address .....	229
13.5 Auto Firmware Upgrade .....	229
<b>Part V: Security .....</b>	<b>231</b>
<b>Chapter 14</b>	
<b>Firewalls.....</b>	<b>233</b>
14.1 Firewall Overview .....	233
14.2 Types of Firewalls .....	233
14.2.1 Packet Filtering Firewalls .....	233
14.2.2 Application-level Firewalls .....	234
14.2.3 Stateful Inspection Firewalls .....	234
14.3 Introduction to ZyXEL's Firewall .....	234
14.3.1 Denial of Service Attacks .....	235
14.4 Denial of Service .....	235
14.4.1 Basics .....	235
14.4.2 Types of DoS Attacks .....	236
14.5 Stateful Inspection .....	238
14.5.1 Stateful Inspection Process .....	239
14.5.2 Stateful Inspection on Your ZyXEL Device .....	240
14.5.3 TCP Security .....	240
14.5.4 UDP/ICMP Security .....	241
14.5.5 Upper Layer Protocols .....	241
14.6 Guidelines for Enhancing Security with Your Firewall .....	242
14.6.1 Security In General .....	242
14.7 Packet Filtering Vs Firewall .....	243
14.7.1 Packet Filtering: .....	243
14.7.2 Firewall .....	243
<b>Chapter 15</b>	
<b>Firewall Configuration .....</b>	<b>245</b>
15.1 Access Methods .....	245
15.2 General Firewall Policy Overview .....	245
15.3 Rule Logic Overview .....	246
15.3.1 Rule Checklist .....	246
15.3.2 Security Ramifications .....	246
15.3.3 Key Fields For Configuring Rules .....	247
15.4 Connection Direction .....	247

## Table of Contents

---

15.4.1 LAN to WAN Rules .....	248
15.4.2 Alerts .....	248
15.5 General Firewall Policy .....	248
15.6 Firewall Rules Summary .....	249
15.6.1 Configuring Firewall Rules .....	251
15.6.2 Customized Services .....	254
15.6.3 Configuring a Customized Service .....	254
15.7 Example Firewall Rule .....	255
15.8 DoS Thresholds .....	259
15.8.1 Threshold Values .....	259
15.8.2 Half-Open Sessions .....	260
15.8.3 Configuring Firewall Thresholds .....	260
15.9 Firewall Commands .....	262
 <b>Chapter 16</b>	
<b>Content Filtering .....</b>	<b>265</b>
16.1 Content Filtering Overview .....	265
16.2 Configuring Keyword Blocking .....	265
16.3 Configuring the Schedule .....	266
16.4 Configuring Trusted Computers .....	267
 <b>Chapter 17</b>	
<b>Introduction to IPSec.....</b>	<b>269</b>
17.1 VPN Overview .....	269
17.1.1 IPSec .....	269
17.1.2 Security Association .....	269
17.1.3 Other Terminology .....	269
17.1.4 VPN Applications .....	270
17.2 IPSec Architecture .....	270
17.2.1 IPSec Algorithms .....	271
17.2.2 Key Management .....	271
17.3 Encapsulation .....	271
17.3.1 Transport Mode .....	272
17.3.2 Tunnel Mode .....	272
17.4 IPSec and NAT .....	272
 <b>Chapter 18</b>	
<b>VPN Screens.....</b>	<b>275</b>
18.1 VPN/IPSec Overview .....	275
18.2 IPSec Algorithms .....	275
18.2.1 AH (Authentication Header) Protocol .....	275
18.2.2 ESP (Encapsulating Security Payload) Protocol .....	275
18.3 My IP Address .....	276

18.4 Secure Gateway Address .....	276
18.4.1 Dynamic Secure Gateway Address .....	277
18.5 VPN Setup Screen .....	277
18.6 Keep Alive .....	279
18.7 VPN, NAT, and NAT Traversal .....	279
18.8 Remote DNS Server .....	280
18.9 ID Type and Content .....	281
18.9.1 ID Type and Content Examples .....	282
18.10 Pre-Shared Key .....	283
18.11 Editing VPN Policies .....	283
18.12 IKE Phases .....	288
18.12.1 Negotiation Mode .....	289
18.12.2 Diffie-Hellman (DH) Key Groups .....	289
18.12.3 Perfect Forward Secrecy (PFS) .....	289
18.13 Configuring Advanced IKE Settings .....	289
18.14 Manual Key Setup .....	292
18.14.1 Security Parameter Index (SPI) .....	292
18.15 Configuring Manual Key .....	292
18.16 Viewing SA Monitor .....	295
18.17 Configuring Global Setting .....	297
18.18 Telecommuter VPN/IPSec Examples .....	297
18.18.1 Telecommuters Sharing One VPN Rule Example .....	297
18.18.2 Telecommuters Using Unique VPN Rules Example .....	298
18.19 VPN and Remote Management .....	300
<b>Chapter 19</b> <b>Certificates .....</b>	<b>301</b>
19.1 Certificates Overview .....	301
19.1.1 Advantages of Certificates .....	302
19.2 Self-signed Certificates .....	302
19.3 Configuration Summary .....	302
19.4 My Certificates .....	303
19.5 My Certificate Import .....	304
19.5.1 Certificate File Formats .....	305
19.6 My Certificate Create .....	306
19.7 My Certificate Details .....	308
19.8 Trusted CAs .....	311
19.9 Trusted CA Import .....	313
19.10 Trusted CA Details .....	314
19.11 Trusted Remote Hosts .....	316
19.12 Verifying a Trusted Remote Host's Certificate .....	318
19.12.1 Trusted Remote Host Certificate Fingerprints .....	318
19.13 Trusted Remote Hosts Import .....	319

## Table of Contents

---

19.14 Trusted Remote Host Certificate Details .....	319
19.15 Directory Servers .....	322
19.16 Directory Server Add and Edit .....	323
<b>Part VI: Advanced .....</b>	<b>325</b>
<b>Chapter 20</b>	
<b>Static Route .....</b>	<b>327</b>
20.1 Static Route .....	327
20.2 Configuring Static Route .....	327
20.2.1 Static Route Edit .....	328
<b>Chapter 21</b>	
<b>Bandwidth Management.....</b>	<b>331</b>
21.1 Bandwidth Management Overview .....	331
21.2 Application-based Bandwidth Management .....	331
21.3 Auto Classifier .....	331
21.4 Subnet-based Bandwidth Management .....	332
21.5 Application and Subnet-based Bandwidth Management .....	333
21.5.1 Bandwidth Management Priorities .....	333
21.6 Configuring Bandwidth Management (General) .....	333
21.7 Bandwidth Management Rule Setup .....	334
21.7.1 Rule Configuration .....	335
21.8 Bandwidth Monitor .....	337
<b>Chapter 22</b>	
<b>Dynamic DNS Setup .....</b>	<b>339</b>
22.1 Dynamic DNS Overview .....	339
22.1.1 DYNDNS Wildcard .....	339
22.2 Configuring Dynamic DNS .....	339
<b>Chapter 23</b>	
<b>Remote Management Configuration .....</b>	<b>343</b>
23.1 Remote Management Overview .....	343
23.1.1 Remote Management Limitations .....	344
23.1.2 Remote Management and NAT .....	344
23.1.3 System Timeout .....	344
23.2 Introduction to HTTPS .....	345
23.3 HTTP .....	346
23.4 Telnet .....	347
23.5 Configuring Telnet .....	347

23.6 Configuring FTP .....	348
23.7 SNMP .....	349
23.7.1 Supported MIBs .....	350
23.7.2 SNMP Traps .....	351
23.7.3 Configuring SNMP .....	351
23.8 Configuring DNS .....	352
23.9 Configuring ICMP .....	353
23.10 SSH .....	354
23.11 How SSH Works .....	355
23.12 SSH Implementation on the ZyXEL Device .....	356
23.12.1 Requirements for Using SSH .....	356
23.13 Configuring SSH .....	356
23.14 Secure Telnet Using SSH Examples .....	357
23.14.1 Example 1: Microsoft Windows .....	357
23.14.2 Example 2: Linux .....	357
23.15 Secure FTP Using SSH Example .....	358
<b>Chapter 24</b>	
<b>Universal Plug-and-Play (UPnP).....</b>	<b>361</b>
24.1 Introducing Universal Plug and Play .....	361
24.1.1 How do I know if I'm using UPnP? .....	361
24.1.2 NAT Traversal .....	361
24.1.3 Cautions with UPnP .....	361
24.2 UPnP and ZyXEL .....	362
24.2.1 Configuring UPnP .....	362
24.3 Installing UPnP in Windows Example .....	363
24.4 Using UPnP in Windows XP Example .....	366
<b>Part VII: Maintenance and Troubleshooting .....</b>	<b>373</b>
<b>Chapter 25</b>	
<b>System .....</b>	<b>375</b>
25.1 General Setup and System Name .....	375
25.1.1 General Setup .....	375
25.2 Time Setting .....	377
<b>Chapter 26</b>	
<b>Call History .....</b>	<b>381</b>
26.1 Call History Overview .....	381
26.2 Viewing the Call History Summary .....	381
26.3 Viewing Call History .....	382

## Table of Contents

---

26.4 Configuring Call History Settings .....	384
<b>Chapter 27</b>	
<b>Logs .....</b>	<b>387</b>
27.1 Logs Overview .....	387
27.1.1 Alerts and Logs .....	387
27.2 Viewing the Logs .....	387
27.3 Configuring Log Settings .....	388
27.4 SMTP Error Messages .....	390
27.4.1 Example E-mail Log .....	391
27.5 Log Descriptions .....	392
<b>Chapter 28</b>	
<b>Troubleshooting.....</b>	<b>401</b>
28.1 Power, Hardware Connections, and LEDs .....	401
28.2 ZyXEL Device Access and Login .....	402
28.3 Internet Access .....	404
28.4 Phone Calls and VoIP .....	405
<b>Chapter 29</b>	
<b>Tools.....</b>	<b>407</b>
29.1 Introduction .....	407
29.2 Filename Conventions .....	407
29.3 File Maintenance Over WAN .....	408
29.4 Firmware Upgrade Screen .....	409
29.5 Backup and Restore .....	410
29.5.1 Backup Configuration .....	411
29.5.2 Restore Configuration .....	411
29.5.3 Reset to Factory Defaults .....	412
29.6 Restart .....	413
29.7 Using FTP or TFTP to Back Up Configuration .....	413
29.7.1 Using the FTP Commands to Back Up Configuration .....	413
29.7.2 FTP Command Configuration Backup Example .....	414
29.7.3 Configuration Backup Using GUI-based FTP Clients .....	414
29.7.4 Backup Configuration Using TFTP .....	414
29.7.5 TFTP Command Configuration Backup Example .....	415
29.7.6 Configuration Backup Using GUI-based TFTP Clients .....	415
29.8 Using FTP or TFTP to Restore Configuration .....	416
29.8.1 Restore Using FTP Session Example .....	416
29.9 FTP and TFTP Firmware and Configuration File Uploads .....	416
29.9.1 FTP File Upload Command from the DOS Prompt Example .....	417
29.9.2 FTP Session Example of Firmware File Upload .....	417
29.9.3 TFTP File Upload .....	417

29.9.4 TFTP Upload Command Example .....	418
<b>Chapter 30</b>	
<b>Diagnostic .....</b>	<b>419</b>
30.1 General Diagnostic .....	419
30.2 DSL Line Diagnostic .....	419
<b>Chapter 31</b>	
<b>Product Specifications .....</b>	<b>423</b>
31.1 Hardware Specifications .....	423
31.2 Firmware Specifications .....	423
31.3 Voice Specifications .....	427
31.4 Wireless Features (Wireless Devices Only) .....	429
31.4.1 IEEE 802.11g Wireless LAN .....	430
31.5 Power Adaptor Specifications .....	431
<b>Part VIII: Appendices and Index .....</b>	<b>433</b>
Appendix A Setting up Your Computer's IP Address.....	435
Appendix B Pop-up Windows, JavaScripts and Java Permissions .....	447
Appendix C IP Addresses and Subnetting .....	453
Appendix D Wireless LANs .....	461
Appendix E Services .....	475
Appendix F Legal Information .....	479
Appendix G Customer Support .....	483
<b>Index.....</b>	<b>489</b>

## Table of Contents

# List of Figures

Figure 1 Internet Access Application .....	43
Figure 2 Internet Telephony Service Provider Application .....	44
Figure 3 Peer-to-peer Calling .....	44
Figure 4 Firewall Application .....	45
Figure 5 LAN-to-LAN Application .....	45
Figure 6 LEDs .....	46
Figure 7 Password Screen .....	50
Figure 8 Change Password Screen .....	51
Figure 9 Replace Certificate Screen .....	51
Figure 10 Wizard or Advanced Screen .....	52
Figure 11 Main Screen .....	52
Figure 12 Select a Mode .....	64
Figure 13 Wizard Welcome .....	64
Figure 14 Auto Detection: No DSL Connection .....	65
Figure 15 Auto-Detection: PPPoE .....	65
Figure 16 Auto Detection: Failed .....	66
Figure 17 Internet Access Wizard Setup: ISP Parameters .....	67
Figure 18 Internet Connection with PPPoE .....	68
Figure 19 Internet Connection with RFC 1483 .....	68
Figure 20 Internet Connection with ENET ENCAP .....	69
Figure 21 Internet Connection with PPPoA .....	70
Figure 22 Connection Test Failed-1 .....	71
Figure 23 Connection Test Failed-2. ....	71
Figure 24 Connection Test Successful .....	72
Figure 25 Wireless LAN Setup Wizard 1 .....	72
Figure 26 Wireless LAN .....	73
Figure 27 Manually Assign a WPA-PSK Key .....	74
Figure 28 Manually Assign a WEP Key .....	74
Figure 29 Wireless LAN Setup 3 .....	75
Figure 30 Internet Access and WLAN Wizard Setup Complete .....	76
Figure 31 VoIP Phone Calls .....	77
Figure 32 Select a Mode .....	78
Figure 33 Wizard: Welcome .....	79
Figure 34 SIP Server Profile Selection .....	79
Figure 35 VoIP Wizard Configuration .....	80
Figure 36 SIP Registration Test .....	81
Figure 37 VoIP Wizard Fail .....	81
Figure 38 VoIP Wizard Finish .....	81

Figure 39 Select a Mode .....	83
Figure 40 Wizard: Welcome .....	84
Figure 41 Bandwidth Management Wizard: General Information .....	84
Figure 42 Bandwidth Management Wizard: Complete .....	85
Figure 43 Status Screen .....	88
Figure 44 Any IP Table .....	91
Figure 45 WLAN Status .....	92
Figure 46 Packet Statistics .....	93
Figure 47 VoIP Statistics .....	94
Figure 48 LED Status .....	96
Figure 49 Example of Traffic Shaping .....	104
Figure 50 Internet Access Setup (PPPoE) .....	106
Figure 51 Advanced Internet Access Setup .....	108
Figure 52 WAN More Connections .....	110
Figure 53 More Connections Edit .....	111
Figure 54 More Connections Edit Advanced .....	113
Figure 55 Traffic Redirect Example .....	114
Figure 56 Traffic Redirect LAN Setup .....	114
Figure 57 WAN Backup Setup .....	115
Figure 58 LAN and WAN IP Addresses .....	117
Figure 59 Any IP Example .....	121
Figure 60 LAN IP .....	122
Figure 61 Advanced LAN Setup .....	123
Figure 62 DHCP Setup .....	124
Figure 63 LAN Client List .....	126
Figure 64 Physical Network & Partitioned Logical Networks .....	127
Figure 65 LAN IP Alias .....	127
Figure 66 Example of a Wireless Network .....	129
Figure 67 Example of a WDS Link .....	132
Figure 68 Wireless LAN: General .....	134
Figure 69 Wireless: No Security .....	135
Figure 70 Wireless: Static WEP Encryption .....	136
Figure 71 Wireless: WPA(2)-PSK .....	137
Figure 72 Wireless: WPA(2) .....	138
Figure 73 Wireless LAN: Advanced .....	139
Figure 74 Network > Wireless LAN > OTIST .....	141
Figure 75 Example: Wireless Client OTIST Screen .....	142
Figure 76 OTIST: Settings .....	142
Figure 77 OTIST: In Progress on the ZyXEL Device .....	142
Figure 78 OTIST: In Progress on the Wireless Device .....	143
Figure 79 Start OTIST? .....	143
Figure 80 MAC Address Filter .....	144
Figure 81 Wireless LAN: Association List .....	145

Figure 82 Wireless LAN: QoS .....	146
Figure 83 Application Priority Configuration .....	147
Figure 84 Wireless LAN > WDS .....	149
Figure 85 Wireless LAN > WDS > Static WEP .....	150
Figure 86 Example: WDS Link using WPA-PSK with TKIP .....	151
Figure 87 Wireless LAN > WDS > WPA-PSK .....	151
Figure 88 Wireless LAN > WDS > WPA2-PSK .....	152
Figure 89 How NAT Works .....	156
Figure 90 NAT Application With IP Alias .....	157
Figure 91 NAT General .....	159
Figure 92 Multiple Servers Behind NAT Example .....	160
Figure 93 Port Forwarding .....	161
Figure 94 Port Forwarding Rule Setup .....	162
Figure 95 Address Mapping Rules .....	163
Figure 96 Edit Address Mapping Rule .....	165
Figure 97 SIP User Agent .....	170
Figure 98 SIP Proxy Server .....	171
Figure 99 SIP Redirect Server .....	172
Figure 100 SIP Call Through Proxy Servers .....	174
Figure 101 DiffServ: Differentiated Service Field .....	177
Figure 102 SIP > SIP Settings .....	178
Figure 103 VoIP > SIP Settings > Advanced .....	180
Figure 104 SIP > QoS .....	183
Figure 105 Phone > Analog Phone .....	186
Figure 106 Phone > Analog Phone > Advanced .....	188
Figure 107 Phone > ISDN Phone .....	190
Figure 108 Phone > Common .....	191
Figure 109 VoIP > Phone > Ext. Table .....	192
Figure 110 VoIP > Phone > Ext. Table > Advanced .....	194
Figure 111 VoIP > Phone > Region .....	198
Figure 112 Phone Book > Speed Dial .....	199
Figure 113 Phone Book > Incoming Call Policy .....	200
Figure 114 Phone Book > Distinctive Ring .....	203
Figure 115 Phone Book > SIP Prefix .....	205
Figure 116 PSTN Line > General .....	206
Figure 117 ISDN Line > General .....	207
Figure 118 VoIP > Fixed Line Numbers Screen .....	210
Figure 119 Peer Devices Connecting .....	212
Figure 120 VoIP Phone To PSTN Phone .....	213
Figure 121 PSTN Phone To VoIP Phone .....	214
Figure 122 PSTN Phone To PSTN Phone via VoIP .....	214
Figure 123 VoIP > Trunking > General .....	214
Figure 124 VoIP > Trunking > Peer Call .....	216

Figure 125 VoIP > Trunking > Call Rule .....	218
Figure 126 VoIP to PSTN Example .....	219
Figure 127 VoIP to PSTN Example - Speed Dial Screen .....	220
Figure 128 VoIP to PSTN Example - Outgoing Authentication .....	220
Figure 129 VoIP to PSTN Example - Incoming Authentication .....	221
Figure 130 PSTN to PSTN Example .....	222
Figure 131 PSTN to PSTN Example: General Configuration .....	223
Figure 132 PSTN to PSTN Example - Outgoing Authentication .....	223
Figure 133 PSTN to PSTN Example - Call Rule .....	224
Figure 134 PSTN to PSTN Example - Incoming Authentication .....	224
Figure 135 Firewall Application .....	235
Figure 136 Three-Way Handshake .....	236
Figure 137 SYN Flood .....	237
Figure 138 Smurf Attack .....	237
Figure 139 Stateful Inspection .....	239
Figure 140 Firewall: General .....	248
Figure 141 Firewall Rules .....	250
Figure 142 Firewall: Edit Rule .....	252
Figure 143 Firewall: Customized Services .....	254
Figure 144 Firewall: Configure Customized Services .....	255
Figure 145 Firewall Example: Rules .....	256
Figure 146 Edit Custom Port Example .....	256
Figure 147 Firewall Example: Edit Rule: Destination Address .....	257
Figure 148 Firewall Example: Edit Rule: Select Customized Services .....	258
Figure 149 Firewall Example: Rules: MyService .....	259
Figure 150 Firewall: Threshold .....	261
Figure 151 Content Filter: Keyword .....	265
Figure 152 Content Filter: Schedule .....	266
Figure 153 Content Filter: Trusted .....	267
Figure 154 Encryption and Decryption .....	270
Figure 155 IPSec Architecture .....	271
Figure 156 Transport and Tunnel Mode IPSec Encapsulation .....	272
Figure 157 IPSec Summary Fields .....	277
Figure 158 VPN Setup .....	278
Figure 159 NAT Router Between IPSec Routers .....	280
Figure 160 VPN Host using Intranet DNS Server Example .....	281
Figure 161 Edit VPN Policies .....	284
Figure 162 Two Phases to Set Up the IPSec SA .....	288
Figure 163 Advanced VPN Policies .....	290
Figure 164 VPN: Manual Key .....	293
Figure 165 VPN: SA Monitor .....	296
Figure 166 VPN: Global Setting .....	297
Figure 167 Telecommuters Sharing One VPN Rule Example .....	298

Figure 168 Telecommuters Using Unique VPN Rules Example .....	299
Figure 169 Certificate Configuration Overview .....	302
Figure 170 My Certificates .....	303
Figure 171 My Certificate Import .....	305
Figure 172 My Certificate Create .....	306
Figure 173 My Certificate Details .....	309
Figure 174 Trusted CAs .....	312
Figure 175 Trusted CA Import .....	313
Figure 176 Trusted CA Details .....	314
Figure 177 Trusted Remote Hosts .....	317
Figure 178 Remote Host Certificates .....	318
Figure 179 Certificate Details .....	318
Figure 180 Trusted Remote Host Import .....	319
Figure 181 Trusted Remote Host Details .....	320
Figure 182 Directory Servers .....	323
Figure 183 Directory Server Add and Edit .....	324
Figure 184 Example of Static Routing Topology .....	327
Figure 185 Static Route .....	328
Figure 186 Static Route Edit .....	329
Figure 187 Subnet-based Bandwidth Management Example .....	332
Figure 188 Bandwidth Management: General .....	333
Figure 189 Bandwidth Management: Rule Setup .....	334
Figure 190 Bandwidth Management Rule Configuration .....	335
Figure 191 Bandwidth Management: Monitor .....	337
Figure 192 Dynamic DNS .....	340
Figure 193 Secure and Insecure Remote Management From the WAN .....	343
Figure 194 HTTPS Implementation .....	345
Figure 195 Remote Management: HTTP .....	346
Figure 196 Telnet Configuration on a TCP/IP Network .....	347
Figure 197 Remote Management: Telnet .....	348
Figure 198 Remote Management: FTP .....	349
Figure 199 SNMP Management Model .....	350
Figure 200 Remote Management: SNMP .....	351
Figure 201 Remote Management: DNS .....	353
Figure 202 Remote Management: ICMP .....	354
Figure 203 SSH Communication Over the WAN Example .....	355
Figure 204 How SSH Works .....	355
Figure 205 ADVANCED > REMOTE MGMT > SSH .....	356
Figure 206 SSH Example 1: Store Host Key .....	357
Figure 207 SSH Example 2: Test .....	358
Figure 208 SSH Example 2: Log in .....	358
Figure 209 Secure FTP: Firmware Upload Example .....	359
Figure 210 Configuring UPnP .....	362

Figure 211 Add/Remove Programs: Windows Setup: Communication .....	363
Figure 212 Add/Remove Programs: Windows Setup: Communication: Components .....	364
Figure 213 Network Connections .....	364
Figure 214 Windows Optional Networking Components Wizard .....	365
Figure 215 Networking Services .....	365
Figure 216 Network Connections .....	366
Figure 217 Internet Connection Properties .....	367
Figure 218 Internet Connection Properties: Advanced Settings .....	368
Figure 219 Internet Connection Properties: Advanced Settings: Add .....	368
Figure 220 System Tray Icon .....	369
Figure 221 Internet Connection Status .....	369
Figure 222 Network Connections .....	370
Figure 223 Network Connections: My Network Places .....	371
Figure 224 Network Connections: My Network Places: Properties: Example .....	371
Figure 225 System General Setup .....	376
Figure 226 System Time Setting .....	377
Figure 227 Call History > Summary .....	382
Figure 228 Call History > Call History .....	383
Figure 229 Call History > Call History Settings .....	384
Figure 230 View Log .....	388
Figure 231 Log Settings .....	389
Figure 232 E-mail Log Example .....	391
Figure 233 Firmware Upgrade .....	409
Figure 234 Firmware Upload In Progress .....	410
Figure 235 Network Temporarily Disconnected .....	410
Figure 236 Error Message .....	410
Figure 237 Configuration .....	411
Figure 238 Configuration Upload Successful .....	412
Figure 239 Network Temporarily Disconnected .....	412
Figure 240 Configuration Upload Error .....	412
Figure 241 Reset Warning Message .....	412
Figure 242 Reset In Process Message .....	413
Figure 243 Restart Screen .....	413
Figure 244 FTP Session Example .....	414
Figure 245 Restore Using FTP Session Example .....	416
Figure 246 FTP Session Example of Firmware File Upload .....	417
Figure 247 Diagnostic: General .....	419
Figure 248 Diagnostic: DSL Line .....	420
Figure 249 WIndows 95/98/Me: Network: Configuration .....	436
Figure 250 Windows 95/98/Me: TCP/IP Properties: IP Address .....	437
Figure 251 Windows 95/98/Me: TCP/IP Properties: DNS Configuration .....	438
Figure 252 Windows XP: Start Menu .....	439
Figure 253 Windows XP: Control Panel .....	439

---

Figure 254 Windows XP: Control Panel: Network Connections: Properties .....	440
Figure 255 Windows XP: Local Area Connection Properties .....	440
Figure 256 Windows XP: Advanced TCP/IP Settings .....	441
Figure 257 Windows XP: Internet Protocol (TCP/IP) Properties .....	442
Figure 258 Macintosh OS 8/9: Apple Menu .....	443
Figure 259 Macintosh OS 8/9: TCP/IP .....	443
Figure 260 Macintosh OS X: Apple Menu .....	444
Figure 261 Macintosh OS X: Network .....	445
Figure 262 Pop-up Blocker .....	447
Figure 263 Internet Options: Privacy .....	448
Figure 264 Internet Options: Privacy .....	449
Figure 265 Pop-up Blocker Settings .....	449
Figure 266 Internet Options: Security .....	450
Figure 267 Security Settings - Java Scripting .....	451
Figure 268 Security Settings - Java .....	451
Figure 269 Java (Sun) .....	452
Figure 270 Network Number and Host ID .....	454
Figure 271 Subnetting Example: Before Subnetting .....	456
Figure 272 Subnetting Example: After Subnetting .....	457
Figure 273 Peer-to-Peer Communication in an Ad-hoc Network .....	461
Figure 274 Basic Service Set .....	462
Figure 275 Infrastructure WLAN .....	463
Figure 276 RTS/CTS .....	464
Figure 277 WPA(2) with RADIUS Application Example .....	471
Figure 278 WPA(2)-PSK Authentication .....	472



# List of Tables

Table 1 Models Covered .....	41
Table 2 LEDs .....	46
Table 3 Web Configurator Icons in the Title Bar .....	53
Table 4 Navigation Panel Summary .....	53
Table 5 Available Features .....	57
Table 6 Internet Access Wizard Setup: ISP Parameters .....	67
Table 7 Internet Connection with PPPoE .....	68
Table 8 Internet Connection with RFC 1483 .....	69
Table 9 Internet Connection with ENET ENCAP .....	69
Table 10 Internet Connection with PPPoA .....	70
Table 11 Wireless LAN Setup Wizard 1 .....	72
Table 12 Wireless LAN Setup Wizard 2 .....	73
Table 13 Manually Assign a WPA key .....	74
Table 14 Manually Assign a WEP key .....	75
Table 15 VoIP Wizard Configuration .....	80
Table 16 Bandwidth Management Wizard: General Information .....	84
Table 17 Status Screen .....	88
Table 18 Any IP Table .....	91
Table 19 WLAN Status .....	92
Table 20 Packet Statistics .....	93
Table 21 VoIP Statistics .....	94
Table 22 LED Status .....	96
Table 23 Internet Access Setup .....	106
Table 24 Advanced Internet Access Setup .....	108
Table 25 Advanced Internet Access Setup .....	110
Table 26 More Connections Edit .....	111
Table 27 More Connections Edit Advanced .....	113
Table 28 WAN Backup Setup .....	115
Table 29 LAN IP .....	122
Table 30 Advanced LAN Setup .....	123
Table 31 DHCP Setup .....	124
Table 32 LAN Client List .....	126
Table 33 LAN IP Alias .....	128
Table 34 Types of Encryption for Each Type of Authentication .....	131
Table 35 Additional Wireless Terms .....	133
Table 36 Wireless LAN: General .....	134
Table 37 Wireless No Security .....	135
Table 38 Wireless: Static WEP Encryption .....	136

Table 39 Wireless: WPA(2)-PSK .....	137
Table 40 Wireless: WPA(2) .....	138
Table 41 Wireless LAN: Advanced .....	140
Table 42 Network > Wireless LAN > OTIST .....	141
Table 43 MAC Address Filter .....	144
Table 44 Wireless LAN: Association List .....	145
Table 45 Wireless LAN: QoS .....	146
Table 46 Application Priority Configuration .....	147
Table 47 Wireless LAN > WDS .....	149
Table 48 Wireless LAN > WDS > Static WEP .....	150
Table 49 Wireless LAN > WDS > WPA-PSK .....	152
Table 50 Wireless LAN > WDS > WPA2-PSK .....	153
Table 51 NAT Definitions .....	155
Table 52 NAT Mapping Types .....	158
Table 53 NAT General .....	159
Table 54 Port Forwarding .....	161
Table 55 Port Forwarding Rule Setup .....	162
Table 56 Address Mapping Rules .....	163
Table 57 Edit Address Mapping Rule .....	165
Table 58 SIP Call Progression .....	173
Table 59 SIP Call Progression .....	174
Table 60 Custom Tones Details .....	176
Table 61 SIP > SIP Settings .....	178
Table 62 VoIP > SIP Settings > Advanced .....	180
Table 63 SIP > QoS .....	183
Table 64 Phone > Analog Phone .....	186
Table 65 Phone > Analog Phone > Advanced .....	188
Table 66 Phone > ISDN Phone .....	190
Table 67 Phone > Common .....	191
Table 68 VoIP > Phone > Ext. Table .....	193
Table 69 VoIP > Phone > Ext. Table > Advanced .....	194
Table 70 European Flash Key Commands .....	195
Table 71 USA Flash Key Commands .....	197
Table 72 VoIP > Phone > Region .....	198
Table 73 Phone Book > Speed Dial .....	199
Table 74 Phone Book > Incoming Call Policy .....	201
Table 75 Phone Book > Distinctive Ring .....	203
Table 76 Phone Book > SIP Prefix .....	205
Table 77 PSTN Line > General .....	207
Table 78 ISDN Line > General .....	207
Table 79 VoIP > Fixed Line Numbers Screen .....	210
Table 80 Matching Incoming and Outgoing Authentication .....	212
Table 81 Call Rules .....	213

Table 82 VoIP > Trunking > General .....	215
Table 83 VoIP > Trunking > Peer Call .....	216
Table 84 VoIP > Trunking > Call Rule .....	218
Table 85 VoIP Trunking Call Progression .....	221
Table 86 PSTN to PSTN: VoIP Trunking Call Progression .....	225
Table 87 Common IP Ports .....	235
Table 88 ICMP Commands That Trigger Alerts .....	238
Table 89 Legal NetBIOS Commands .....	238
Table 90 Legal SMTP Commands .....	238
Table 91 Firewall: General .....	249
Table 92 Firewall Rules .....	250
Table 93 Firewall: Edit Rule .....	252
Table 94 Customized Services .....	254
Table 95 Firewall: Configure Customized Services .....	255
Table 96 Firewall: Threshold .....	261
Table 97 Sys Firewall Commands .....	262
Table 98 Content Filter: Keyword .....	266
Table 99 Content Filter: Schedule .....	267
Table 100 Content Filter: Trusted .....	267
Table 101 VPN and NAT .....	273
Table 102 AH and ESP .....	276
Table 103 VPN Setup .....	278
Table 104 VPN and NAT .....	280
Table 105 Local ID Type and Content Fields .....	282
Table 106 Peer ID Type and Content Fields .....	282
Table 107 Matching ID Type and Content Configuration Example .....	282
Table 108 Mismatching ID Type and Content Configuration Example .....	283
Table 109 Edit VPN Policies .....	284
Table 110 Advanced VPN Policies .....	290
Table 111 VPN: Manual Key .....	293
Table 112 VPN: SA Monitor .....	296
Table 113 VPN: Global Setting .....	297
Table 114 Telecommuters Sharing One VPN Rule Example .....	298
Table 115 Telecommuters Using Unique VPN Rules Example .....	299
Table 116 My Certificates .....	303
Table 117 My Certificate Import .....	305
Table 118 My Certificate Create .....	306
Table 119 My Certificate Details .....	310
Table 120 Trusted CAs .....	312
Table 121 Trusted CA Import .....	313
Table 122 Trusted CA Details .....	315
Table 123 Trusted Remote Hosts .....	317
Table 124 Trusted Remote Host Import .....	319

Table 125 Trusted Remote Host Details .....	321
Table 126 Directory Servers .....	323
Table 127 Directory Server Add and Edit .....	324
Table 128 Static Route .....	328
Table 129 Static Route Edit .....	329
Table 130 Typical Packet Sizes .....	332
Table 131 Automatic Traffic Classifier Priorities .....	332
Table 132 Application and Subnet-based Bandwidth Management Example .....	333
Table 133 Bandwidth Management Priorities .....	333
Table 134 Bandwidth Management: General .....	334
Table 135 Bandwidth Management: Rule Setup .....	334
Table 136 Bandwidth Management Rule Configuration .....	336
Table 137 Dynamic DNS .....	340
Table 138 Remote Management: HTTP .....	346
Table 139 Remote Management: Telnet .....	348
Table 140 Remote Management: FTP .....	349
Table 141 SNMP Traps .....	351
Table 142 Remote Management: SNMP .....	352
Table 143 Remote Management: DNS .....	353
Table 144 Remote Management: ICMP .....	354
Table 145 ADVANCED > REMOTE MGMT > SSH .....	356
Table 146 Configuring UPnP .....	362
Table 147 System General Setup .....	376
Table 148 System Time Setting .....	377
Table 149 Call History > Summary .....	382
Table 150 Call History > Call History .....	383
Table 151 Call History > Call History Settings .....	385
Table 152 View Log .....	388
Table 153 Log Settings .....	389
Table 154 SMTP Error Messages .....	391
Table 155 System Maintenance Logs .....	392
Table 156 System Error Logs .....	393
Table 157 Access Control Logs .....	393
Table 158 TCP Reset Logs .....	393
Table 159 Packet Filter Logs .....	394
Table 160 ICMP Logs .....	394
Table 161 CDR Logs .....	394
Table 162 PPP Logs .....	395
Table 163 UPnP Logs .....	395
Table 164 Content Filtering Logs .....	395
Table 165 Attack Logs .....	395
Table 166 802.1X Logs .....	396
Table 167 ACL Setting Notes .....	397

---

Table 168 ICMP Notes .....	397
Table 169 Syslog Logs .....	398
Table 170 SIP Logs .....	398
Table 171 RTP Logs .....	399
Table 172 FSM Logs: Caller Side .....	399
Table 173 FSM Logs: Callee Side .....	399
Table 174 PSTN Logs .....	399
Table 175 RFC-2408 ISAKMP Payload Types .....	400
Table 176 Filename Conventions .....	408
Table 177 Firmware Upgrade .....	409
Table 178 Restore Configuration .....	411
Table 179 General Commands for GUI-based FTP Clients .....	414
Table 180 General Commands for GUI-based TFTP Clients .....	415
Table 181 Diagnostic: General .....	419
Table 182 Diagnostic: DSL Line .....	420
Table 183 Hardware Specifications .....	423
Table 184 Firmware Specifications .....	423
Table 185 Voice Features .....	427
Table 186 Wireless Features .....	429
Table 187 IEEE 802.11g .....	430
Table 188 P-2602HWL Series Power Adaptor Specifications .....	431
Table 189 Subnet Masks .....	454
Table 190 Subnet Masks .....	455
Table 191 Maximum Host Numbers .....	455
Table 192 Alternative Subnet Mask Notation .....	455
Table 193 Subnet 1 .....	457
Table 194 Subnet 2 .....	458
Table 195 Subnet 3 .....	458
Table 196 Subnet 4 .....	458
Table 197 Eight Subnets .....	458
Table 198 24-bit Network Number Subnet Planning .....	459
Table 199 16-bit Network Number Subnet Planning .....	459
Table 200 IEEE 802.11g .....	465
Table 201 Wireless Security Levels .....	466
Table 202 Comparison of EAP Authentication Types .....	469
Table 203 Wireless Security Relational Matrix .....	472
Table 204 Examples of Services .....	475



---

# PART I

# Introduction

---

[Introducing the ZyXEL Device \(41\)](#)

[Introducing the Web Configurator \(49\)](#)



# Introducing the ZyXEL Device

This chapter introduces the main applications and features of the ZyXEL Device. It also introduces the ways you can manage the ZyXEL Device.

## 1.1 Overview

The ZyXEL Device is an Integrated Access Device (IAD) that combines an ADSL2+ router with Voice over IP (VoIP) communication capabilities to allow you to use a traditional analog or ISDN telephone to make Internet calls. By integrating DSL and NAT, you are provided with ease of installation and high-speed, shared Internet access. The ZyXEL Device is also a complete security solution with a robust firewall and content filtering.

At the time of writing, this guide covers the following models.

**Table 1** Models Covered

P-2602HWNLI-D3A
P-2602HWNLI-D7A

- In the ZyXEL Device product name, “H” denotes an integrated 4-port switch (hub).
- “W” denotes wireless functionality. There is an embedded mini-PCI module for IEEE 802.11g wireless LAN connectivity.
- “N” denotes the ability to connect an ISDN (Integrated Services Digital Network) telephone to the device.
- “L” denotes the PSTN (Public Switched Telephone Network) line feature.




---

When the ZyXEL Device does not have power, only the phone connected to the **PHONE 1** port can be used for making calls. Ensure you know which phone this is, so that in case of emergency you can make outgoing calls.

---

- “I” denotes the ISDN (Integrated Services Digital Network) line feature.<sup>1</sup>

---

1. A device that includes both “L” and “I” in the model name can support either a PSTN line or a ISDN line, but not both at the same time.

The P-2602HWNLI-D3A works over ISDN (Integrated Services Digital Network).

The P-2602HWNLI-D7A works over T-ISDN (UR-2).



---

Only use firmware for your ZyXEL Device's specific model. Refer to the label on the bottom of your ZyXEL Device.

---

The web browser-based Graphical User Interface (GUI) provides easy management. See the appendix on Product Specifications for a full list of features.

## 1.2 Ways to Manage the ZyXEL Device

Use any of the following methods to manage the ZyXEL Device.

- Web Configurator. This is recommended for everyday management of the ZyXEL Device using a (supported) web browser.
- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers.
- FTP for firmware upgrades and configuration backup/restore.
- SNMP. The device can be monitored by an SNMP manager. See the SNMP chapter in this User's Guide.
- SPTGEN. SPTGEN is a text configuration file that allows you to configure the device by uploading an SPTGEN file. This is especially convenient if you need to configure many devices of the same type.
- Vantage CNM (Centralized Network Management). The device can be remotely managed using a Vantage CNM server.
- TR-069. This is an auto-configuration server used to remotely configure your device.

## 1.3 Good Habits for Managing the ZyXEL Device

Do the following things regularly to make the ZyXEL Device more secure and to manage the ZyXEL Device more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the ZyXEL Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the ZyXEL Device. You could simply restore your last configuration.

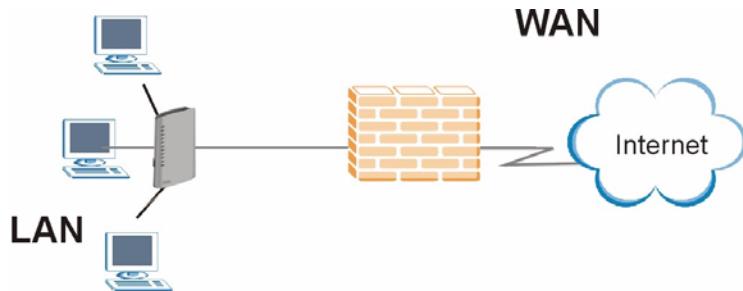
## 1.4 Applications for the ZyXEL Device

Here are some example uses for which the ZyXEL Device is well suited.

### 1.4.1 Internet Access

Your device is the ideal high-speed Internet access solution. It supports the TCP/IP protocol, which the Internet uses exclusively. It is compatible with all major ADSL DSLAM (Digital Subscriber Line Access Multiplexer) providers. A DSLAM is a rack of ADSL line cards with data multiplexed into a backbone network interface/connection (for example, T1, OC3, DS3, ATM or Frame Relay). Think of it as the equivalent of a modem rack for ADSL. In addition, your device allows wireless clients access to your network resources and the Internet. A typical Internet access application is shown below.

**Figure 1** Internet Access Application



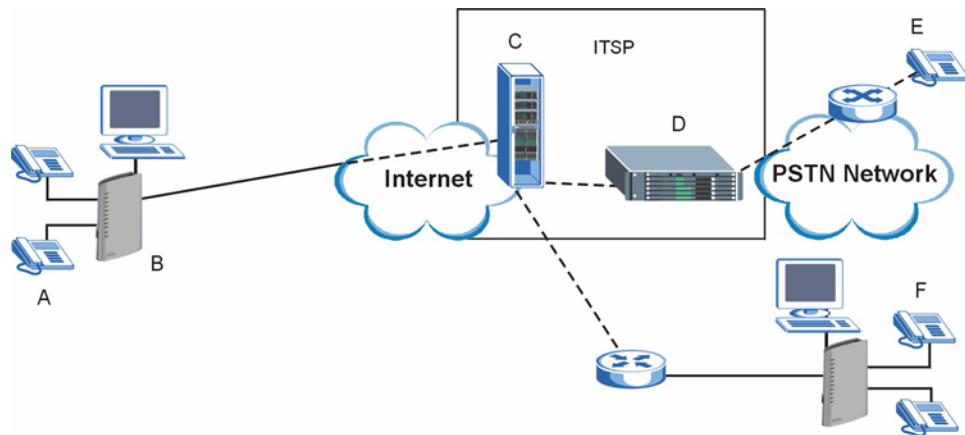
#### 1.4.1.1 Internet Single User Account

For a SOHO (Small Office/Home Office) environment, your device offers the Single User Account (SUA) feature that allows multiple users on the LAN (Local Area Network) to access the Internet concurrently for the cost of a single IP address

### 1.4.2 Making Calls via Internet Telephony Service Provider

In a home or small office environment, you can use your device to make and receive VoIP telephone calls through an Internet Telephony Service Provider (ITSP).

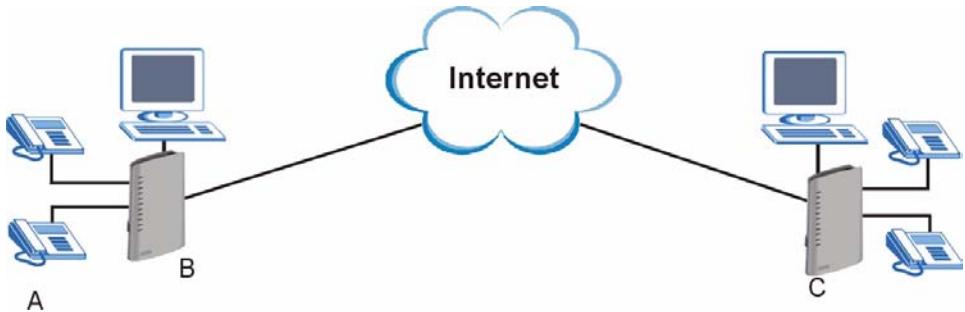
The following figure shows a basic example of how you would make a VoIP call through an ITSP. You use your analog phone (**A** in the figure) and your device (**B**) changes the call into VoIP. Your device then sends your call to the Internet and the ITSP's SIP server (**C**). The VoIP call server forwards calls to PSTN phones (**E**) through a trunking gateway (**D**) to the PSTN network. The VoIP call server forwards calls to IP phones (**F**) through the Internet.

**Figure 2** Internet Telephony Service Provider Application

### 1.4.3 Make Peer-to-peer Calls

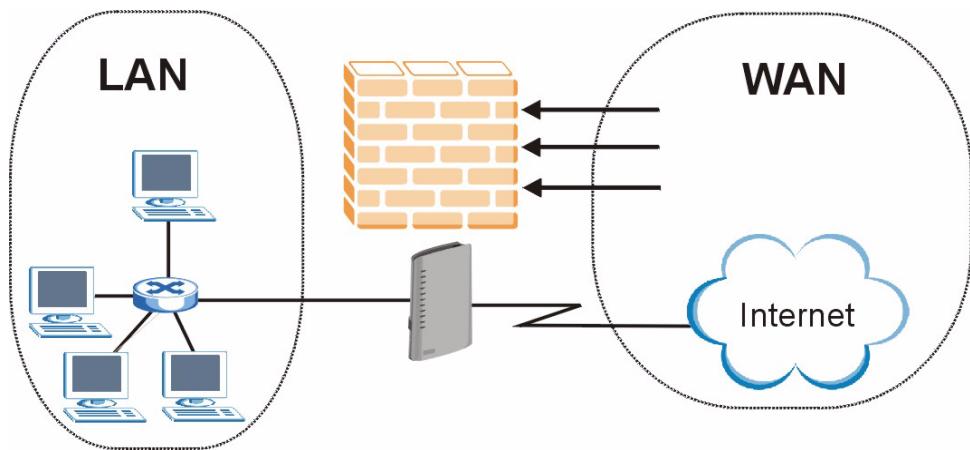
You can call directly to someone's IP address without using a SIP proxy server. Peer-to-peer calls are also called "Point to Point" or "IP-to-IP" calls. You must know the peer's IP address in order to do this.

The following figure shows a basic example of how you would make a peer-to-peer VoIP call. You use your analog phone (A in the figure) and your device (B) changes the call into VoIP. and sends the call through the Internet to the peer VoIP device (C).

**Figure 3** Peer-to-peer Calling

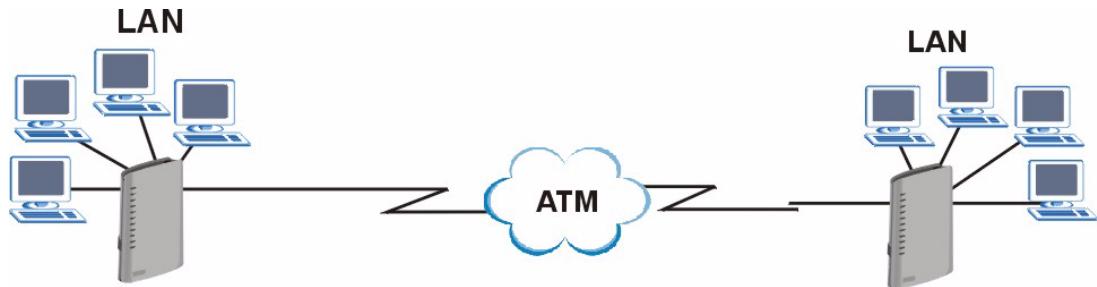
### 1.4.4 Firewall for Secure Broadband Internet Access

Your device provides protection from attacks by Internet hackers. By default, the firewall blocks all incoming traffic from the WAN. The firewall supports TCP/UDP inspection and DoS (Denial of Services) detection and prevention, as well as real time alerts, reports and logs.

**Figure 4** Firewall Application

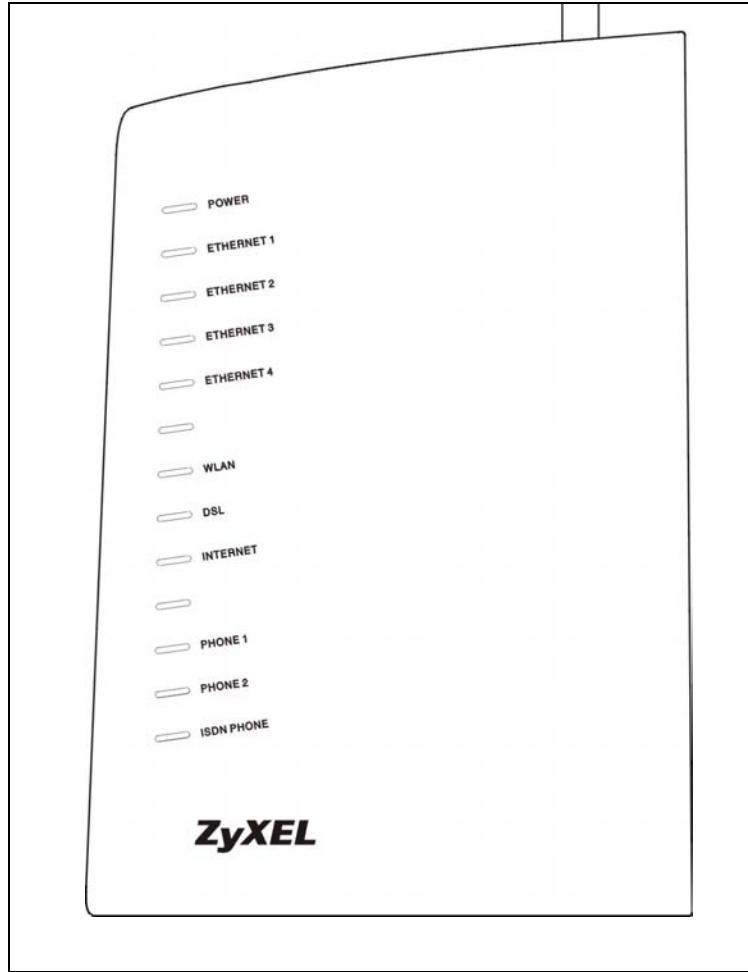
#### 1.4.5 LAN to LAN Application

You can use your device to connect two geographically dispersed networks over the ADSL line. A typical LAN-to-LAN application is shown as follows.

**Figure 5** LAN-to-LAN Application

## 1.5 LEDs

**Figure 6** LEDs



The following table describes your device's LEDs.

**Table 2** LEDs

LED	COLOR	STATUS	DESCRIPTION
<b>POWER</b>	Green	On	Your device is receiving power and functioning properly.
		Blinking	Your device is rebooting and performing a self-test.
	Red	On	Your device is not ready or there is a malfunction.
	None	Off	Your device is not turned on.
<b>ETHERNET 1-4</b>	Green	On	Your device has a successful Ethernet connection.
		Blinking	The ZyXEL Device is sending/receiving data.
	None	Off	The Ethernet port is not connected.
<b>WLAN</b>	Green	On	Your device is ready, but is not sending/receiving data through the wireless LAN.
		Blinking	Your device is sending/receiving data through the wireless LAN.
	None	Off	The wireless LAN is not ready or has failed.

**Table 2** LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
<b>DSL</b>	Green	On	Your device has a DSL connection.
		Blinking	Your device is initializing the DSL line.
	None	Off	The DSL link is down.
<b>INTERNET</b>	Green	On	Your device has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the DSL connection is up.
		Blinking	Your device is sending or receiving IP traffic.
	Red	On	Your device attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
	None	Off	Your device does not have an IP connection
<b>PHONE 1, 2</b>	Green	On	A SIP account is registered for the phone port.
		Blinking	A telephone connected to the phone port has its receiver off of the hook or there is an incoming call.
	Orange	On	A SIP account is registered for the phone port and there is a voice message in the corresponding SIP account.
		Blinking	A telephone connected to the phone port has its receiver off of the hook and there is a voice message in the corresponding SIP account.
	None	Off	The phone port does not have a SIP account registered.
<b>ISDN PHONE</b>	Green	On	A SIP account is registered for the phone port.
		Blinking	A telephone connected to the phone port has its receiver off of the hook or there is an incoming call.
	None	Off	The phone port does not have a SIP account registered.

Refer to the Quick Start Guide for information on hardware connections.

## 1.6 The RESET Button

You can use the **RESET** button at the back of the device to turn the wireless LAN off or on. You can also use it to activate OTIST in order to assign your wireless security settings to wireless clients. If you forget your password or cannot access the web configurator, you will need to use the **RESET** button to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to “1234”. You can also use the

### 1.6.1 Using The Reset Button

- 1 Make sure the **POWER** LED is on (not blinking).
- 2 Do one of the following.

To turn the wireless LAN off or on, press the **RESET** button for one second and release it. The **WLAN** LED should change from on to off or vice versa. (“W” models only)

To activate OTIST in order to assign your wireless security settings to wireless clients, press the **RESET** button for five seconds and release it. The **WLAN** LED should flash while the device uses OTIST to send wireless settings to OTIST clients. (“W” models only)

To set the device back to the factory default settings, press the **RESET** button for ten seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

# Introducing the Web Configurator

This chapter describes how to access and navigate the web configurator.

## 2.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy device setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

See [Appendix B on page 447](#) if you need to make sure these functions are allowed in Internet Explorer.

### 2.1.1 Accessing the Web Configurator

- 1 Make sure your ZyXEL Device hardware is properly connected (refer to the Quick Start Guide).
- 2 Launch your web browser.
- 3 Type "192.168.1.1" as the URL.
- 4 A password screen displays.

**Figure 7** Password Screen

## 2.2 Login Types

There are two login types; “user” and “administrator”. When you choose user access, you can make basic configuration changes only. Advanced features are not available. When you choose administrator access, all features are available. See [Chapter 2 on page 57](#) for more information.

### 2.2.1 User Access

- 1 For user access, type the default user name **user** and default user password **1234** in the password screen to enter the user mode.
- 2 If you haven’t changed the password yet, you can just click **Login**. Click **Cancel** to revert to the default password in the password field. If you have changed the password, enter your password and click **Login**.
- 3 Follow steps (from step 3) in [Section 2.2.2 on page 50](#).



---

The default user name and password are case-sensitive.

---

### 2.2.2 Administrator Access

- 1 For administrator access, type the default user name **admin** and the default admin password **admin** in the password screen to configure the advanced features.
- 2 Click **Login** to proceed to a screen asking you to change your password or click **Cancel** to revert to the default password.
- 3 The following screen displays if you have not yet changed your password. It is strongly recommended you change the default password. Enter a new password, retype it to confirm and click **Apply**; alternatively click **Ignore** to proceed to the main menu if you do not want to change the password now.



If you do not change the password, the following screen appears every time you log in with the default password.

**Figure 8** Change Password Screen

Use this screen to change the password.

Your router is currently using the default password. To protect your network from unauthorized users we suggest you change your password at this time. Please select a new password that will be easy to remember yet difficult for others to guess. We suggest you combine text with numbers to make it more difficult for an intruder to guess.

Enter your new password in the two fields below and click "Apply". Otherwise click "Ignore" to keep the default password

New Password:

Retype to Confirm:

Apply      Ignore

- Click **Apply** in the Replace Certificate screen to create a certificate using your ZyXEL Device's MAC address that will be specific to this device. This screen displays only when you log in as an administrator.

**Figure 9** Replace Certificate Screen

Replace Factory Default Certificate

The factory default certificate is common to all ZyXEL models. Click Apply to create a certificate using your ZyXEL's MAC address that will be specific to this device.

Apply      Ignore

- A screen displays to let you choose whether to go to the wizard or the advanced screens.
  - Click **Go to Wizard setup** if you are logging in for the first time or if you want to make basic changes. The wizard selection screen appears after you click **Apply**. See [Chapter 3 on page 63](#) for more information.
  - Click **Go to Advanced setup** if you want to configure features that are not available in the wizards. Select the check box if you always want to go directly to the advanced screens. The main screen appears after you click **Apply**. See [Section 2.3 on page 52](#) for more information.
  - Click **Exit** if you want to log out.



For security reasons, the ZyXEL Device automatically logs you out if you do not use the web configurator for five minutes (default). If this happens, log in again.

**Figure 10** Wizard or Advanced Screen



## 2.3 Web Configurator Main Screen

**Figure 11** Main Screen

**A** ZyXEL

**B** Status

**C**

**D**

**Main Screen Description:**

- A (Header):** Shows the ZyXEL logo and navigation links: Status, VoIP, Security, Advanced, Maintenance, System, Logs, Configuration, and Troubleshooting.
- B (Left Sidebar):** Shows the device model (P-2602HWNLI-D7A) and a tree view of configuration categories: Network, VoIP, Security, Advanced, Maintenance, System, Logs, Configuration, and Troubleshooting.
- C (Central Content Area):**
  - Status:** Refresh Interval dropdown, Apply button.
  - Device Information:** Host Name: P-2602HWNLI-D7A, Model Number: P-2602HWNLI-D7A, MAC Address: 00:13:49:81:1e:65, Zyxos Firmware Version: V3.40(ADV.3)b2 | 03/06/2007, DSL Firmware Version: T1 AR7 07.00.04.00. WAN Information: DSL Mode: NORMAL, IP Address: 0.0.0.0, IP Subnet Mask: 0.0.0.0, Default Gateway: N/A, VPI/VCI: 1/32. LAN Information: IP Address: 192.168.1.1, IP Subnet Mask: 255.255.255.0, DHCP: Server. WLAN Information: SSID: ZyXEL, Channel: 6, Security: Disable. Security: Firewall: Enabled, Content Filter: Disable.
  - System Status:** System Uptime: 2:38:44, Current Date/Time: 01/01/2000 02:40:57, System Mode: Routing / Bridging, CPU Usage: 10.17%, Memory Usage: 48%.
  - Interface Status:** Interface: DSL (Down, 0 kbps / 0 kbps), LAN (Up, 100M/Full Duplex), WLAN (Active, 54M).
  - Summary:** Client List, AnyIP Table, WLAN Status, Bandwidth Status, VPN Status, Packet Statistics, VoIP Statistics, LED Status.
- D (Bottom Status Bar):** Shows VoIP Status: Account (SIP 1, SIP 2), Registration (Register, Register Fail), URI (ChangeMe@profile1.zyxel.com.tw), and a message "Ready".

As illustrated above, the main screen is divided into these parts:

- **A** - title bar
- **B** - navigation panel
- **C** - main window
- **D** - status bar

### 2.3.1 Title Bar

The title bar allows you to change the language and provides some icons in the upper right corner.



The icons provide the following functions.

**Table 3** Web Configurator Icons in the Title Bar

ICON	DESCRIPTION
	<b>Help:</b> Click this icon to open up help screens.
	<b>Wizards:</b> Click this icon to go to the configuration wizards. See <a href="#">Chapter 3 on page 63</a> for more information.
	<b>Logout:</b> Click this icon to log out of the web configurator.

### 2.3.2 Navigation Panel

Use the menu items on the navigation panel to configure ZyXEL Device features. When a user logs in, only basic menu items display. When an administrator logs in, all menu items display for configuration. See [Chapter 2 on page 57](#) for more information.

The following tables describe each menu item.

**Table 4** Navigation Panel Summary

LINK	TAB	FUNCTION
Status		This screen contains administrative and system-related information.
Network		
WAN	Internet Access Setup	Use this screen to configure ISP parameters, WAN IP address assignment, DNS servers and other advanced properties.
	More Connections	Use this screen to configure additional WAN connections.
	WAN Backup Setup	Use this screen to configure a backup gateway.
LAN	IP	Use this screen to configure LAN TCP/IP settings, enable Any IP and other advanced properties.
	DHCP Setup	Use this screen to configure LAN DHCP settings.
	Client List	Use this screen to view current DHCP client information and to always assign specific IP addresses to individual MAC addresses (and host names).
	IP Alias	Use this screen to partition your LAN interface into subnets.

**Table 4** Navigation Panel Summary

LINK	TAB	FUNCTION
Wireless LAN	General	Use this screen to configure the wireless LAN settings and WLAN authentication/security settings.
	OTIST	Use this screen to assign your wireless security settings to wireless clients.
	MAC Filter	Use this screen to configure the ZyXEL Device to give exclusive access to specific wireless clients or exclude specific wireless clients from accessing the ZyXEL Device.
	Association List	Use this screen to view the wireless stations that are currently associated with the ZyXEL Device. You can also block the individual wireless station from accessing the ZyXEL Device.
	QoS	WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of individual services.
	WDS	Use this screen to set up your WDS (Wireless Distribution System) links between the ZyXEL Device and other wireless APs.
NAT	General	Use this screen to enable NAT.
	Port Forwarding	Use this screen to make your local servers visible to the outside world.
VoIP		
SIP	SIP Settings	Use this screen to configure your ZyXEL Device's Voice over IP settings.
	QoS	Use this screen to configure your ZyXEL Device's Quality of Service settings for VoIP.
Phone	Analog Phone	Use this screen to set which <b>Phone 1</b> and <b>Phone 2</b> port settings.
	ISDN Phone	Use this screen to configure the ISDN phone port settings.
	Common	Use this screen to configure general phone port settings.
	Ext. Table	Use this screen to configure extension numbers of the phone ports.
	Region	Use this screen to select your location and call service mode.
Phone Book	Speed Dial	Use this screen to configure speed dial for SIP phone numbers that you call often.
	Incoming Call Policy	Use this screen to configure call-forwarding.
	Distinctive Ring	Use this screen to configure ring tone behavior based on the origin of incoming calls.
	SIP Prefix	Use this screen to set up numbers you dial to select a SIP account for outgoing calls.
PSTN Line	General	Use this screen to configure your ZyXEL Device's settings for PSTN calls.
ISDN Line	General	Use this screen to configure your ZyXEL Device's settings for ISDN calls.
Fixed Line Numbers	Fixed Line Numbers	Use this screen to allow your ISDN phone to receive PSTN calls. You can also use this screen to allow your analog phone(s) to make and receive calls over the ISDN line using Multiple Subscriber Numbers (MSNs).
Trunking	General	Use this screen to enable trunking on your ZyXEL Device.
	Peer Call	Use this screen to configure peer device authentication for trunking calls.
	Call Rule	Use this screen to configure forwarding rules on your ZyXEL Device for trunking calls.
Security		

**Table 4** Navigation Panel Summary

LINK	TAB	FUNCTION
Firewall	General	Use this screen to activate/deactivate the firewall and the default action to take on network traffic going in specific directions.
	Rules	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule.
	Threshold	Use this screen to configure the thresholds for determining when to drop sessions that do not become fully established.
Content Filter	Keyword	Use this screen to block access to web sites containing certain keywords in the URL.
	Schedule	Use this screen to set the days and times for your device to perform content filtering.
	Trusted	Use this screen to exclude a range of users on the LAN from content filtering.
VPN	Setup	Use this screen to configure each VPN tunnel.
	Monitor	Use this screen to look at the current status of each VPN tunnel.
	VPN Global Setting	Use this screen to allow NetBIOS traffic through VPN tunnels.
Certificates	My Certificates	Use this screen to generate and export self-signed certificates or certification requests and import the ZyXEL Device's CA-signed certificates.
	Trusted CAs	Use this screen to save CA certificates to the ZyXEL Device.
	Trusted Remote Hosts	Use this screen to import self-signed certificates.
	Directory Servers	Use this screen to configure a list of addresses of directory servers (that contain lists of valid and revoked certificates).
Advanced		
Static Route	Static Route	Use this screen to configure IP static routes to tell your device about networks beyond the directly connected remote nodes.
Bandwidth MGMT	General	Use this screen to configure bandwidth management on an interface.
	Rule Setup	Use this screen to define a bandwidth rule.
	Monitor	Use this screen to view the ZyXEL Device's bandwidth usage and allotments.
Dynamic DNS	Dynamic DNS	This screen allows you to use a static hostname alias for a dynamic IP address.

**Table 4** Navigation Panel Summary

LINK	TAB	FUNCTION
Remote MGMT	HTTP	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP and HTTPS to manage the ZyXEL Device.
	Telnet	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the ZyXEL Device.
	FTP	Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the ZyXEL Device.
	SNMP	Use this screen to configure your ZyXEL Device's settings for Simple Network Management Protocol management.
	DNS	Use this screen to configure through which interface(s) and from which IP address(es) users can send DNS queries to the ZyXEL Device.
	ICMP	Use this screen to set whether or not your ZyXEL Device will respond to pings and probes for services that you have not made available.
	SSH	Use this screen to configure through which interface(s) and from which IP address(es) users can use Secure Shell to manage the ZyXEL Device.
UPnP	General	Use this screen to turn UPnP on or off.
Maintenance		
System	General	Use this screen to configure your device's name, domain name, management inactivity timeout and password.
	Time Setting	Use this screen to change your ZyXEL Device's time and date.
Logs	View Log	Use this screen to display your device's logs.
	Log Settings	Use this screen to select which logs and/or immediate alerts your device is to record. You can also set it to e-mail the logs to you.
Call History	Summary	Use this screen to display duration and packet statistics about calls made and received on the ZyXEL Device.
	Call History	Use this screen to display information about individual incoming and outgoing calls.
	Call History Settings	Use this screen to configure to where the ZyXEL Device is to send call history records and the schedule for when the ZyXEL Device is to save and send the records.
Tools	Firmware	Use this screen to upload firmware to your device.
	Configuration	Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings.
	Restart	This screen allows you to reboot the ZyXEL Device without turning the power off.
Diagnostic	General	Use this screen to test the connections to other devices.
	DSL Line	These screen displays information to help you identify problems with the DSL connection.

### 2.3.2.1 Available Features for User and Administrator

The following table lists the features respectively available for user and administrator access. An “O” indicates that a feature is available in this mode.

**Table 5 Available Features**

LINK	FEATURE	USER	ADMINISTRATOR
Internet/Wireless Setup Wizard		O	O
VoIP Setup Wizard		O	O
Bandwidth Management Wizard		O	O
System Statistics		O	O
Network			
WAN	Internet Access Setup	O	O
	More Connections		O
	WAN Backup Setup		O
LAN	IP		O
	DHCP Setup		O
	Client List		O
	IP Alias		O
Wireless LAN	General	O	O
	OTIST	O	O
	MAC Filter		O
	Association List		O
	QoS		O
	WDS		O
NAT	General		O
	Port Forwarding	O	O
VoIP			
SIP	SIP Settings	O	O
	QoS		O
Phone	Analog Phone	O	O
	ISDN Phone		O
	Common	O	O
	Ext. Table	O	O
	Region	O	O
Phone Book	Speed Dial	O	O
	Incoming Call Policy		O
	Distinctive Ring		O
	SIP Prefix	O	O
PSTN Line	General	O	O
ISDN Line	General	O	O

**Table 5** Available Features

LINK	FEATURE	USER	ADMINISTRATOR
Fixed Line Numbers	Fixed Line Numbers	O	O
Trunking	General		O
	Peer Call		O
	Call Rule		O
Security			
Firewall	General	O	O
	Rules		O
	Threshold		O
Content Filter	Keyword		O
	Schedule		O
	Trusted		O
VPN	Setup		O
	Monitor		O
	VPN Global Setting		O
Certificates	My Certificates		O
	Trusted CAs		O
	Trusted Remote Hosts		O
	Directory Servers		O
Advanced			
Static Route	Static Route		O
Bandwidth MGMT	General	O	O
	Rule Setup		O
	Monitor	O	O
Dynamic DNS	Dynamic DNS		O
Remote MGMT	HTTP		O
	Telnet		O
	FTP		O
	SNMP		O
	DNS		O
	ICMP		O
	SSH		O
UPnP	General	O	O
Maintenance			O
System	General	O	O
	Time Setting	O	O
Logs	View Log	O	O
	Log Settings	O	O

**Table 5** Available Features

LINK	FEATURE	USER	ADMINISTRATOR
Call History	Summary		O
	Call History		O
	Call History Settings		O
Tools	Firmware	O	O
	Configuration	O	O
	Restart	O	O
Diagnostic	General		O
	DSL Line		O

### 2.3.3 Main Window

The main window displays information and configuration fields. It is discussed in the rest of this document.

Right after you log in, the **Status** screen is displayed. See [Chapter 6 on page 87](#) for more information about the **Status** screen.

### 2.3.4 Status Bar

Check the status bar when you click **Apply** or **OK** to verify that the configuration has been updated.



---

# PART II

# Wizards and Status

---

Internet and Wireless Setup Wizard (63)

VoIP Wizard (77)

Bandwidth Management Wizard (83)

Status Screens (87)



# Internet and Wireless Setup Wizard

This chapter provides information on the Wizard Setup screens for Internet access in the web configurator.

## 3.1 Introduction

Use the wizard setup screens to configure your system for Internet access with the information given to you by your ISP.



---

See the advanced menu chapters for background information on these fields.

---

## 3.2 Internet Access Wizard Setup

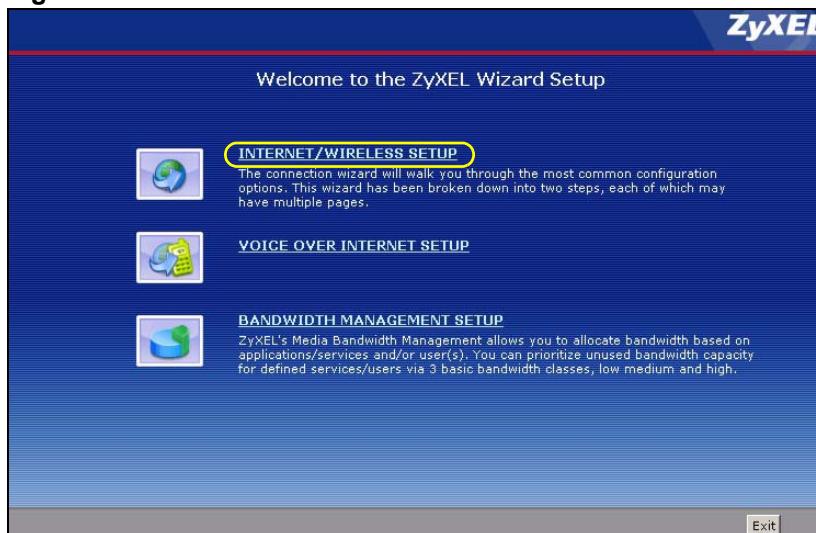
- 1 After you enter the password to access the web configurator, select **Go to Wizard setup** and click **Apply**. Otherwise, click the wizard icon ( in the top right corner of the web configurator to go to the wizards.

**Figure 12** Select a Mode



- 2** Click **INTERNET/WIRELESS SETUP** to configure the system for Internet access and wireless connection.

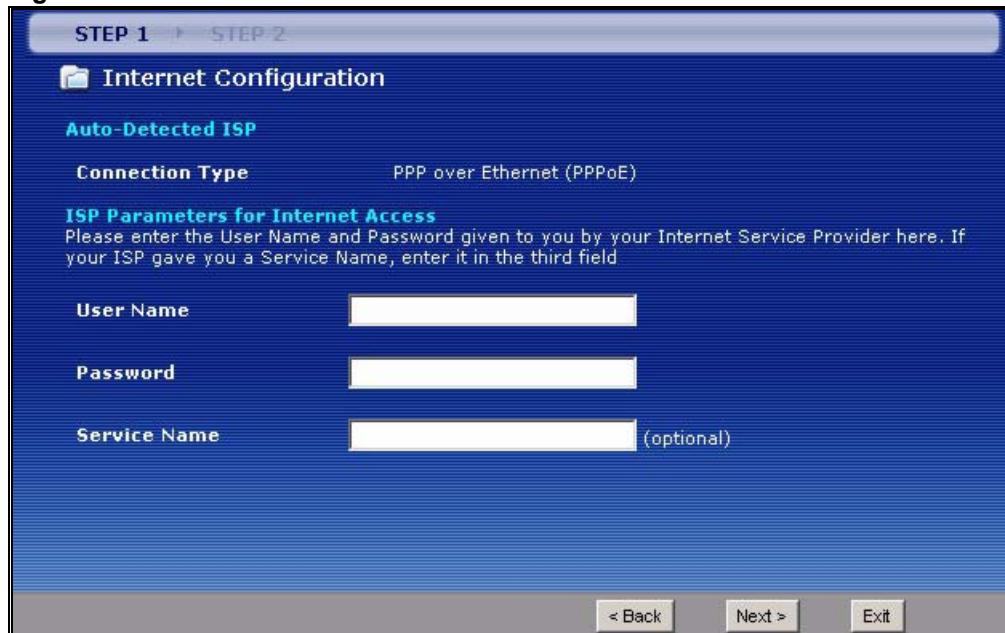
**Figure 13** Wizard Welcome



- 3** Your ZyXEL device attempts to detect your DSL connection and your connection type.
- 3a** The following screen appears if a connection is not detected. Check your hardware connections and click **Restart the Internet/Wireless Setup Wizard** to return to the wizard welcome screen. If you still cannot connect, click **Manually configure your Internet connection**. Follow the directions in the wizard and enter your Internet setup information as provided to you by your ISP. See [Section 3.2.1 on page 66](#) for more details.
- If you would like to skip your Internet setup and configure the wireless LAN settings, leave **Yes** selected and click **Next**.

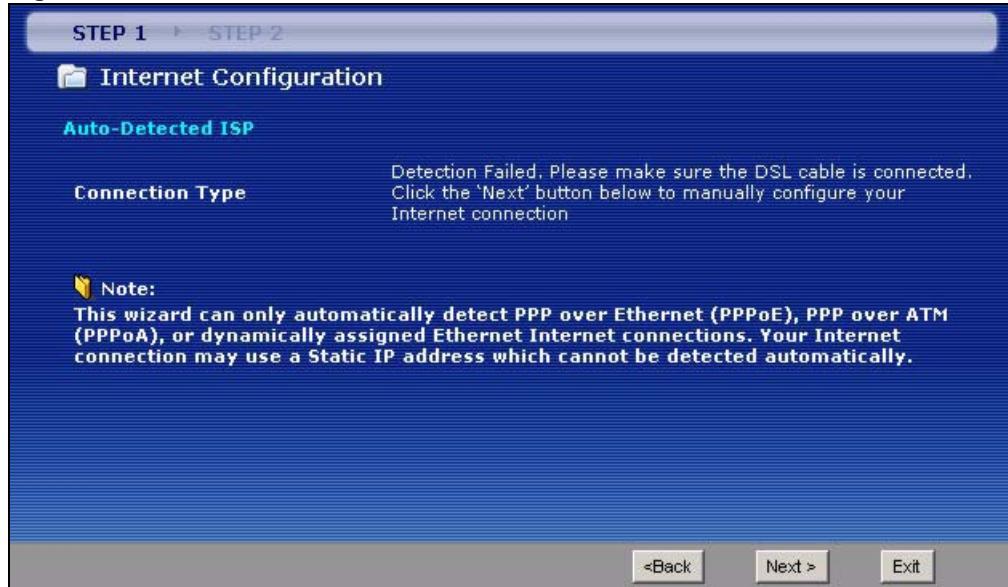
**Figure 14** Auto Detection: No DSL Connection

**3b** The following screen displays if a PPPoE or PPPoA connection is detected. Enter your Internet account information (username, password and/or service name) exactly as provided by your ISP. Then click **Next** and see [Section 3.3 on page 71](#) for wireless connection wizard setup.

**Figure 15** Auto-Detection: PPPoE

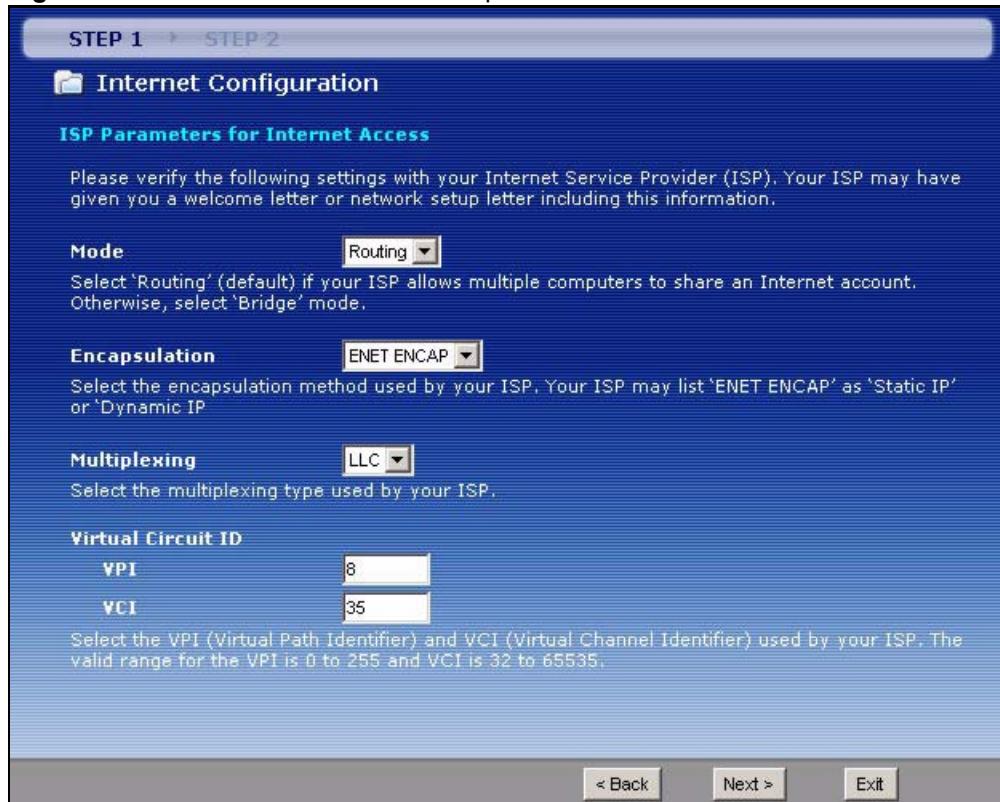
**3c** The following screen appears if the ZyXEL device detects a connection but not the connection type. Click **Next** and refer to [Section 3.2.1 on page 66](#) on how to manually configure the ZyXEL Device for Internet access.

**Figure 16** Auto Detection: Failed



### 3.2.1 Manual Configuration

- 1 If the ZyXEL Device fails to detect your DSL connection type but the physical line is connected, enter your Internet access information in the wizard screen exactly as your service provider gave it to you. Leave the defaults in any fields for which you were not given information.

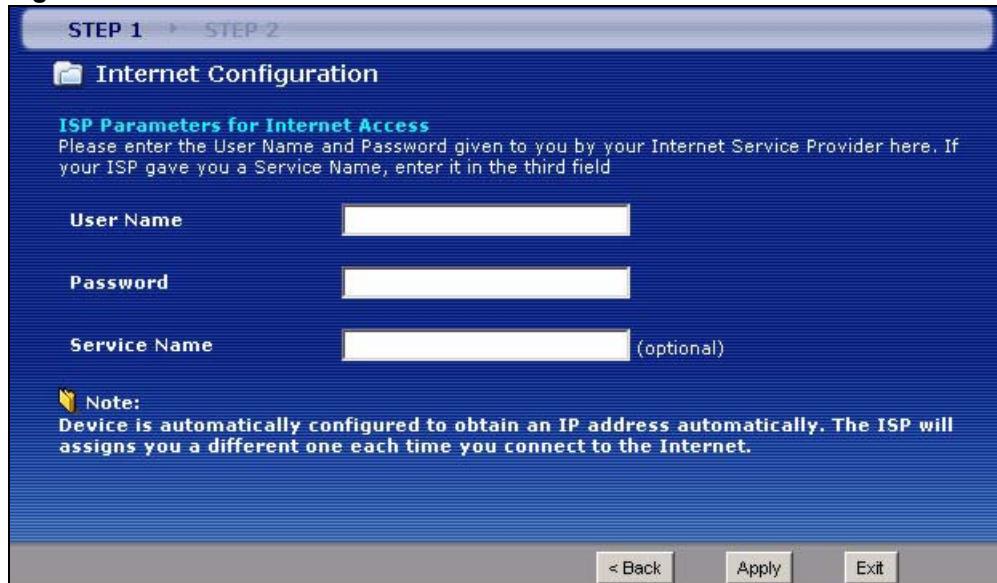
**Figure 17** Internet Access Wizard Setup: ISP Parameters

The following table describes the fields in this screen.

**Table 6** Internet Access Wizard Setup: ISP Parameters

LABEL	DESCRIPTION
Mode	From the <b>Mode</b> drop-down list box, select <b>Routing</b> (default) if your ISP allows multiple computers to share an Internet account. Otherwise select <b>Bridge</b> .
Encapsulation	Select the encapsulation type your ISP uses from the <b>Encapsulation</b> drop-down list box. Choices vary depending on what you select in the <b>Mode</b> field. If you select <b>Bridge</b> in the Mode field, select either <b>PPPoA</b> or <b>RFC 1483</b> . If you select <b>Routing</b> in the Mode field, select <b>PPPoA</b> , <b>RFC 1483</b> , <b>ENET ENCAP</b> or <b>PPPoE</b> .
Multiplexing	Select the multiplexing method used by your ISP from the <b>Multiplex</b> drop-down list box either VC-based or LLC-based.
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	Enter the VPI assigned to you. This field may already be configured.
VCI	Enter the VCI assigned to you. This field may already be configured.
Back	Click <b>Back</b> to go back to the previous screen.
Next	Click <b>Next</b> to continue to the next wizard screen. The next wizard screen you see depends on what protocol you chose above.
Exit	Click <b>Exit</b> to close the wizard screen without saving your changes.

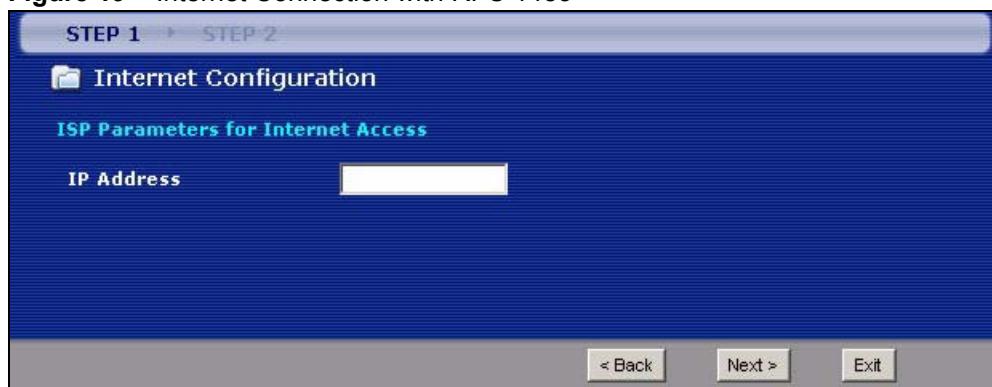
- 2 The next wizard screen varies depending on what mode and encapsulation type you use. All screens shown are with routing mode. Configure the fields and click **Next** to continue. See [Section 3.3 on page 71](#) for wireless connection wizard setup

**Figure 18** Internet Connection with PPPoE

The following table describes the fields in this screen.

**Table 7** Internet Connection with PPPoE

LABEL	DESCRIPTION
User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
Service Name	Type the name of your PPPoE service here.
Back	Click <b>Back</b> to go back to the previous wizard screen.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Exit	Click <b>Exit</b> to close the wizard screen without saving your changes.

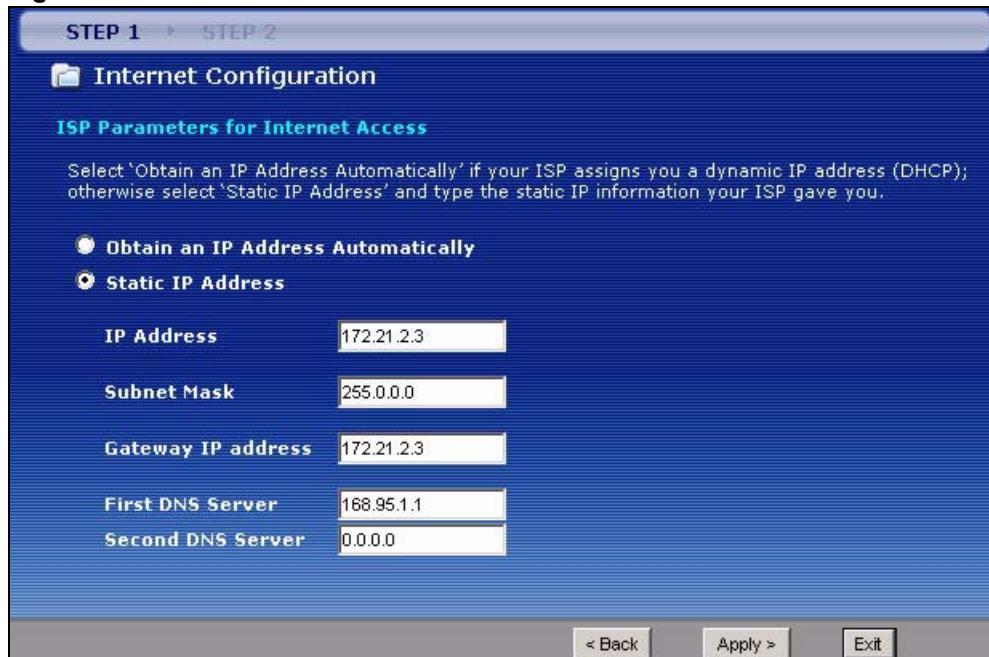
**Figure 19** Internet Connection with RFC 1483

The following table describes the fields in this screen.

**Table 8** Internet Connection with RFC 1483

LABEL	DESCRIPTION
IP Address	This field is available if you select <b>Routing</b> in the <b>Mode</b> field. Type your ISP assigned IP address in this field.
Back	Click <b>Back</b> to go back to the previous wizard screen.
Next	Click <b>Next</b> to continue to the next wizard screen.
Exit	Click <b>Exit</b> to close the wizard screen without saving your changes.

**Figure 20** Internet Connection with ENET ENCAP



The following table describes the fields in this screen.

**Table 9** Internet Connection with ENET ENCAP

LABEL	DESCRIPTION
Obtain an IP Address Automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select <b>Obtain an IP Address Automatically</b> if you have a dynamic IP address.
Static IP Address	Select <b>Static IP Address</b> if your ISP gave you an IP address to use.
IP Address	Enter your ISP assigned IP address.
Subnet Mask	Enter a subnet mask in dotted decimal notation. Refer to the appendix to calculate a subnet mask If you are implementing subnetting.
Gateway IP address	You must specify a gateway IP address (supplied by your ISP) when you use <b>ENET ENCAP</b> in the <b>Encapsulation</b> field in the previous screen.
First DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Second DNS Server	As above.
Back	Click <b>Back</b> to go back to the previous wizard screen.

**Table 9** Internet Connection with ENET ENCAP (continued)

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Exit	Click <b>Exit</b> to close the wizard screen without saving your changes.

**Figure 21** Internet Connection with PPPoA

The following table describes the fields in this screen.

**Table 10** Internet Connection with PPPoA

LABEL	DESCRIPTION
User Name	Enter the login name that your ISP gives you.
Password	Enter the password associated with the user name above.
Back	Click <b>Back</b> to go back to the previous wizard screen.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Exit	Click <b>Exit</b> to close the wizard screen without saving your changes.

- If the user name and/or password you entered for PPPoE or PPPoA connection are not correct, the screen displays as shown next. Click **Back to Username and Password setup** to go back to the screen where you can modify them.

**Figure 22** Connection Test Failed-1

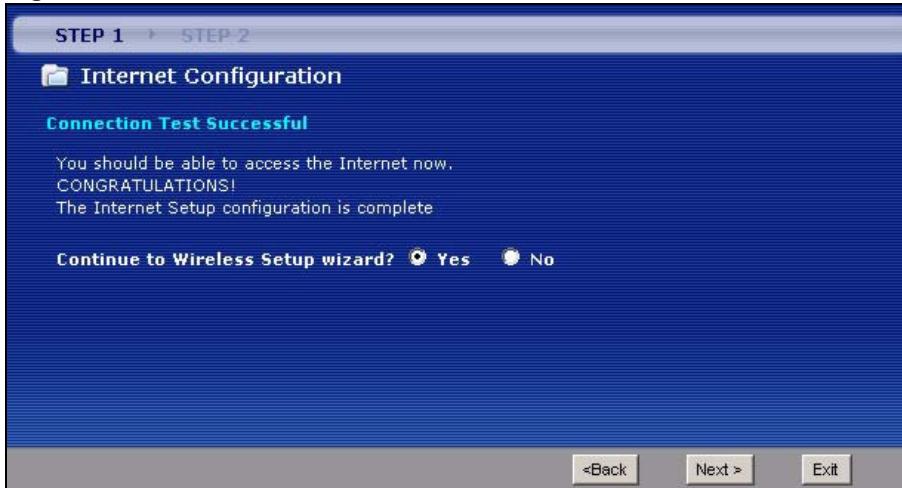
- If the following screen displays, check if your account is activated or click **Restart the Internet/Wireless Setup Wizard** to verify your Internet access settings.

**Figure 23** Connection Test Failed-2.

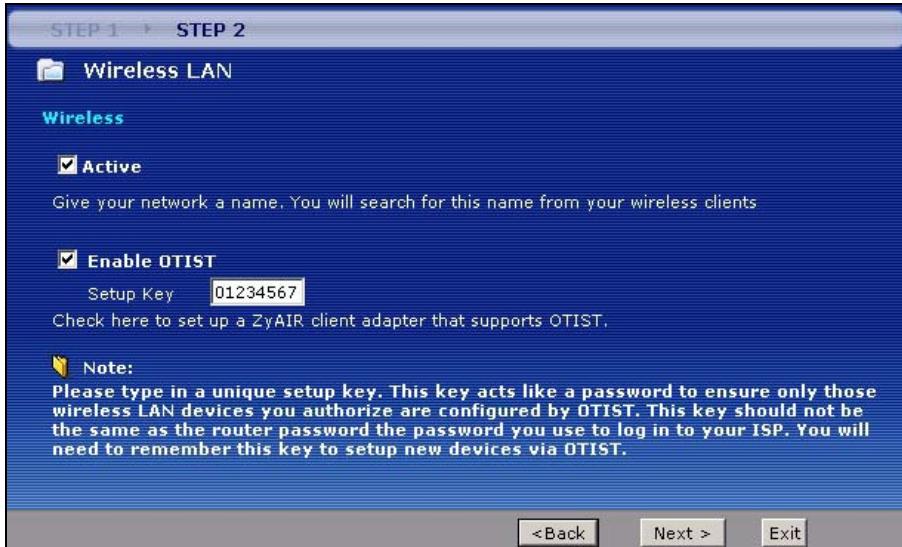
### 3.3 Wireless Connection Wizard Setup

After you configure the Internet access information, use the following screens to set up your wireless LAN.

- 1 Select **Yes** and click **Next** to configure wireless settings. Otherwise, select **No** and skip to Step 6.

**Figure 24** Connection Test Successful

**2** Use this screen to activate the wireless LAN and OTIST. Click **Next** to continue.

**Figure 25** Wireless LAN Setup Wizard 1

The following table describes the labels in this screen.

**Table 11** Wireless LAN Setup Wizard 1

LABEL	DESCRIPTION
Active	Select the check box to turn on the wireless LAN.
Enable OTIST	Select the check box to enable OTIST if you want to transfer your ZyXEL Device's SSID and WEP or WPA-PSK security settings to wireless clients that support OTIST and are within transmission range. You must also activate and start OTIST on the wireless client at the same time. The process takes three minutes to complete.
Setup Key	Type an OTIST <b>Setup Key</b> of up to eight ASCII characters in length. Be sure to use the same OTIST <b>Setup Key</b> on the ZyXEL Device and wireless clients.
Back	Click <b>Back</b> to display the previous screen.
Next	Click <b>Next</b> to proceed to the next screen.
Exit	Click <b>Exit</b> to close the wizard screen without saving.

- 3** Configure your wireless settings in this screen. Click **Next**.

**Figure 26** Wireless LAN



The following table describes the labels in this screen.

**Table 12** Wireless LAN Setup Wizard 2

LABEL	DESCRIPTION
Network Name(SSID)	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the ZyXEL Device, make sure all wireless stations use the same SSID in order to access the network.
Channel Selection	The range of radio frequencies used by IEEE 802.11b/g wireless devices is called a channel. Select a channel ID that is not already in use by a neighboring device.
Security	Select <b>Automatically assign a WPA key (Recommended)</b> to have the ZyXEL Device create a pre-shared key (WPA-PSK) automatically only if your wireless clients support WPA and OTIST. This option is available only when you enable OTIST in the previous wizard screen. Select <b>Manually assign a WPA-PSK key</b> to configure a Pre-Shared Key (WPA-PSK). Choose this option only if your wireless clients support WPA. See <a href="#">Section 3.3.1 on page 74</a> for more information. Select <b>Manually assign a WEP key</b> to configure a WEP Key. See <a href="#">Section 3.3.2 on page 74</a> for more information. Select <b>Disable wireless security</b> to have no wireless LAN security configured. Your network is accessible to any wireless networking device that is within range.
Back	Click <b>Back</b> to display the previous screen.
Next	Click <b>Next</b> to proceed to the next screen.
Exit	Click <b>Exit</b> to close the wizard screen without saving.



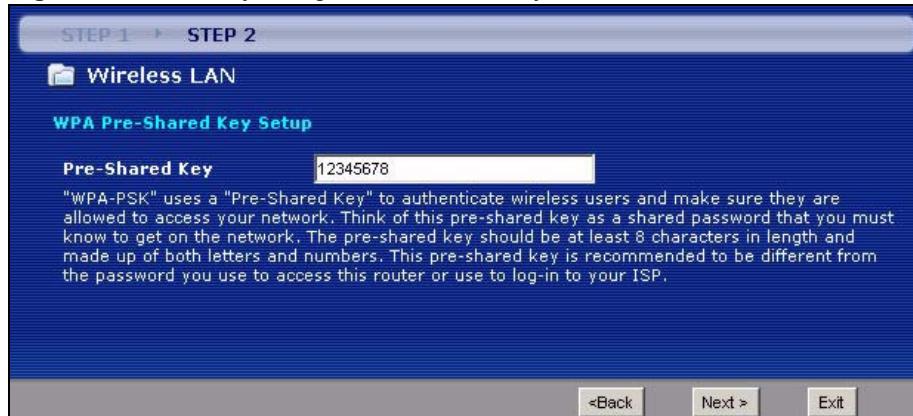
The wireless stations and ZyXEL Device must use the same SSID, channel ID and WEP encryption key (if WEP is enabled), WPA-PSK (if WPA-PSK is enabled) for wireless communication.

- 4** This screen varies depending on the security mode you selected in the previous screen. Fill in the field (if available) and click **Next**.

### 3.3.1 Manually Assign a WPA-PSK Key

Choose **Manually assign a WPA-PSK key** in the Wireless LAN setup screen to set up a **Pre-Shared Key**.

**Figure 27** Manually Assign a WPA-PSK Key



The following table describes the labels in this screen.

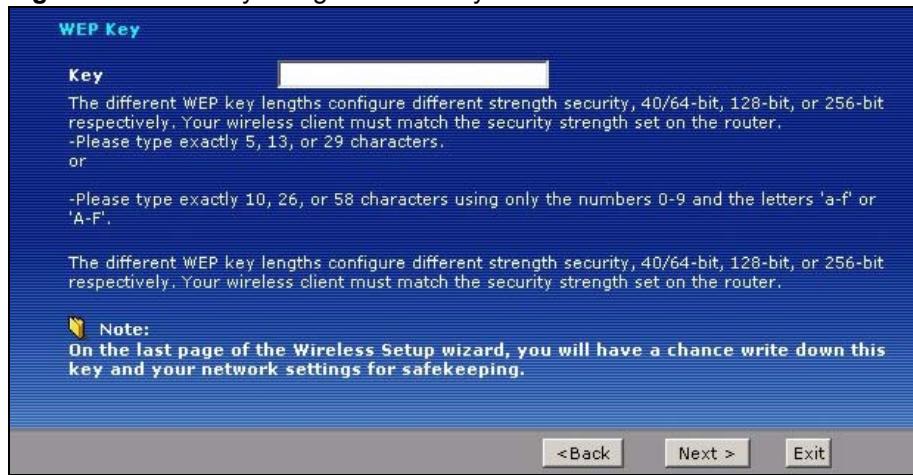
**Table 13** Manually Assign a WPA key

LABEL	DESCRIPTION
Pre-Shared Key	Type from 8 to 63 case-sensitive ASCII characters. You can set up the most secure wireless connection by configuring WPA in the wireless LAN screens. You need to configure an authentication server to do this.
Back	Click <b>Back</b> to display the previous screen.
Next	Click <b>Next</b> to proceed to the next screen.
Exit	Click <b>Exit</b> to close the wizard screen without saving.

### 3.3.2 Manually Assign a WEP Key

Choose **Manually assign a WEP key** to setup WEP Encryption parameters.

**Figure 28** Manually Assign a WEP Key



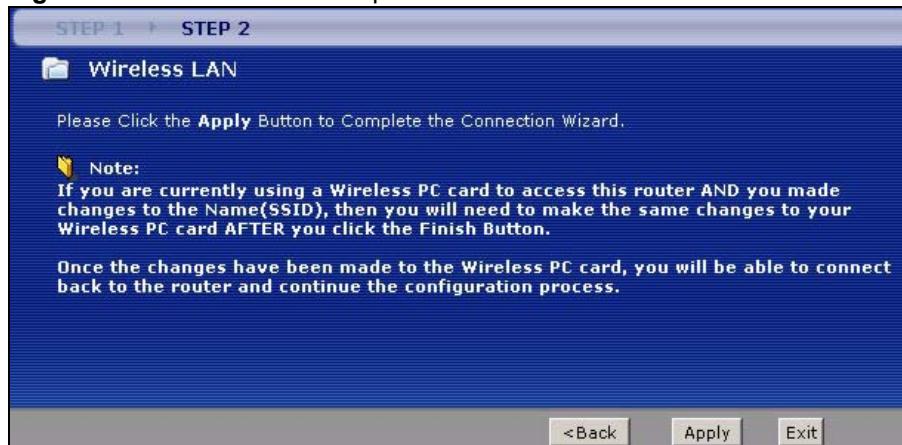
The following table describes the labels in this screen.

**Table 14** Manually Assign a WEP key

LABEL	DESCRIPTION
Key	The WEP keys are used to encrypt data. Both the ZyXEL Device and the wireless stations must use the same WEP key for data transmission. Enter any 5, 13 or 29 ASCII characters or 10, 26 or 58 hexadecimal characters ("0-9", "A-F") for a 64-bit, 128-bit or 256-bit WEP key respectively.
Back	Click <b>Back</b> to display the previous screen.
Next	Click <b>Next</b> to proceed to the next screen.
Exit	Click <b>Exit</b> to close the wizard screen without saving.

- 5** Click **Apply** to complete your wireless LAN settings.

**Figure 29** Wireless LAN Setup 3



- 6** Use the read-only summary table to check whether what you have configured is correct.  
Click **Finish** to complete and save the wizard setup.




---

No wireless LAN settings display if you chose not to configure wireless LAN settings.

---

**Figure 30** Internet Access and WLAN Wizard Setup Complete



- 7 Launch your web browser and navigate to [www.zyxel.com](http://www.zyxel.com). Internet access is just the beginning. Refer to the rest of this guide for more detailed information on the complete range of ZyXEL Device features. If you cannot access the Internet, open the web configurator again to confirm that the Internet settings you configured in the wizard setup are correct.

# VoIP Wizard

This chapter shows you how to configure and register your SIP account(s).

## 4.1 Introduction

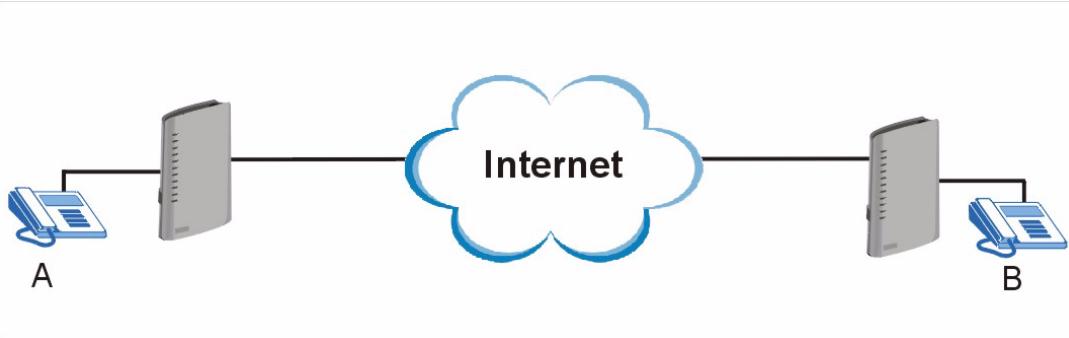
The ZyXEL Device has Voice over IP (VoIP) communication capabilities that allow you to use a traditional analog or ISDN telephone to make Internet calls. This section describes how you can set up your ZyXEL Device to call someone who is also using a VoIP device. You can configure the ZyXEL Device to use up to two SIP-based VoIP accounts.



The ZyXEL Device provides ten SIP accounts although you can configure only 2 via the VoIP wizard. See [Chapter 11 on page 178](#) to configure the others.

In the following figure, **A** represents your phone and **B** represents the phone of the person you would like to call.

**Figure 31** VoIP Phone Calls



In order to make VoIP calls you need to register at least one SIP account on your ZyXEL Device. You can register your SIP account in the VoIP Setup Wizard.

## 4.2 VoIP Wizard Setup

Use the wizard setup screens to set up your SIP account with the information given to you by your ISP and register your SIP account.



Make sure you have a successful Internet connection before you run the VoIP wizard. To test your Internet connection, you can open your web browser and go to any web page (for example, <http://www.zyxel.com>).

---

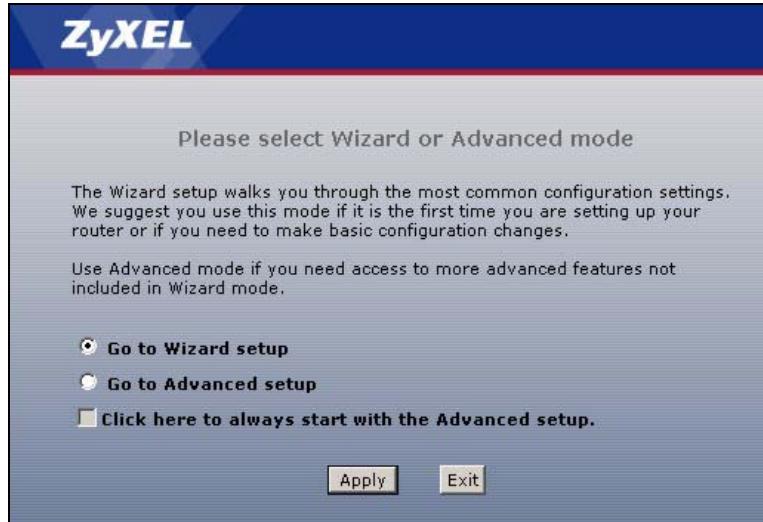


You must have a SIP account before you setup the VoIP wizard.

---

- 1 After you enter the password to access the web configurator, select **Go to Wizard setup** and click **Apply**. Otherwise, click the wizard icon (  ) in the top right corner of the web configurator to display the wizard main screen.

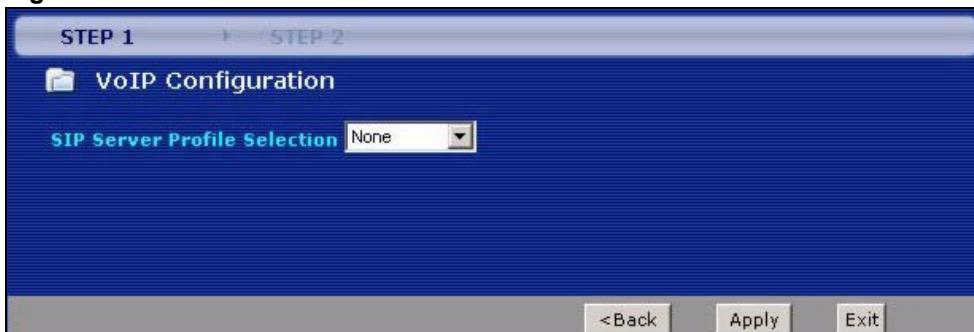
**Figure 32** Select a Mode



- 2 Click **VOICE OVER INTERNET SETUP** to configure your SIP settings.

**Figure 33** Wizard: Welcome

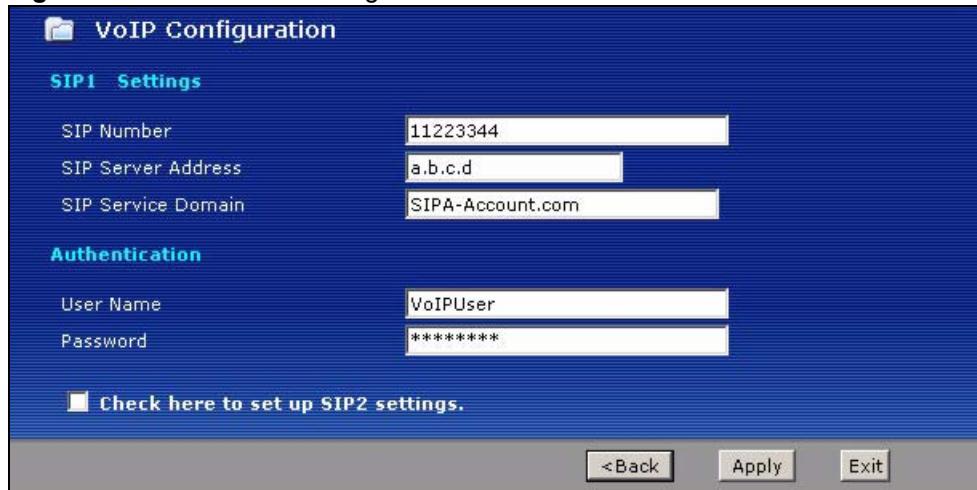
- 3** Select the SIP server profile of your VoIP service provider, either **SIP Profile 1** or **SIP Profile 2**, and click **Apply**. If your VoIP service provider is not in the list, select **None** and click **Apply**.

**Figure 34** SIP Server Profile Selection

- 4** Fill in the fields with the information provided by your VoIP service provider. When you are finished, click **Apply**. Contact your VoIP service provider if you do not have this information.



If your selected a preconfigured SIP profile, just enter your SIP number, user name and password. Leave the remaining fields at default.

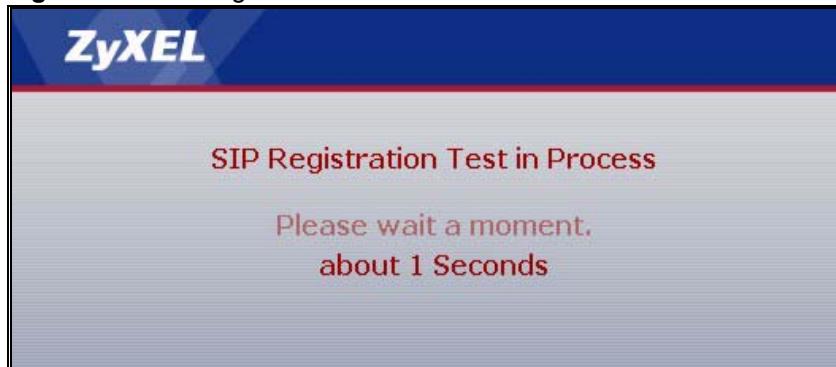
**Figure 35** VoIP Wizard Configuration

The following table describes the labels in this screen.

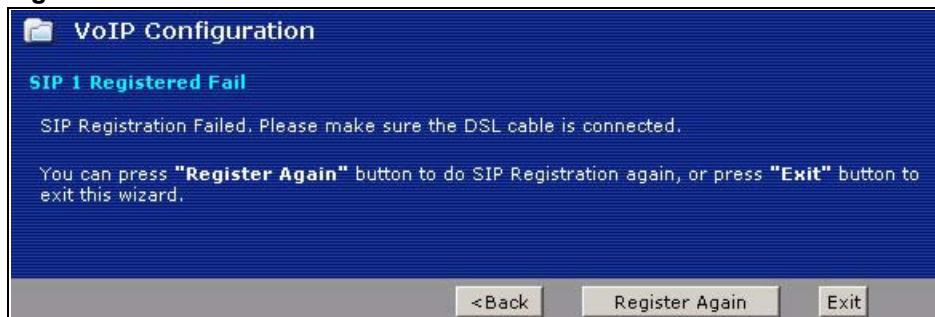
**Table 15** VoIP Wizard Configuration

LABEL	DESCRIPTION
SIP Number	Enter your SIP number in this field. Use the number or text that comes before the @ symbol in a SIP account. If your SIP account is <a href="mailto:11223344@SIPA-Account.com">11223344@SIPA-Account.com</a> , your SIP number is “11223344”. You can use up to 127 ASCII characters.
SIP Server Address	Type the IP address or domain name of the SIP server in this field in dotted decimal notation (for example 192.168.3.1). It doesn’t matter whether the SIP server is a proxy, redirect or register server. You can use up to 95 ASCII characters.
SIP Service Domain	Enter the SIP service domain name in this field (the domain name that comes after the @ symbol in a SIP account like <a href="mailto:11223344@SIPA-Account.com">11223344@SIPA-Account.com</a> ). You can use up to 127 ASCII Extended set characters.
User Name	This is the username you use to login to your SIP account and to register this SIP account with the SIP register server. Type the user name exactly as it was given to you. You can use up to 95 ASCII characters.
Password	Type the password associated with the user name above. You can use up to 95 ASCII Extended set characters.
Check here to set up SIP2 settings.	<p>This screen configures SIP account 1. Select the check box if you have a second SIP account that you want to use. You will need to configure the same fields for the second SIP account.</p> <p>Note: If you configure more than one SIP account, you need to configure <b>Analog Phone</b> settings to distinguish between the two accounts when you make and receive phone calls.</p>
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to complete the wizard setup and save your configuration.
Exit	Click <b>Exit</b> to close the wizard without saving your settings.

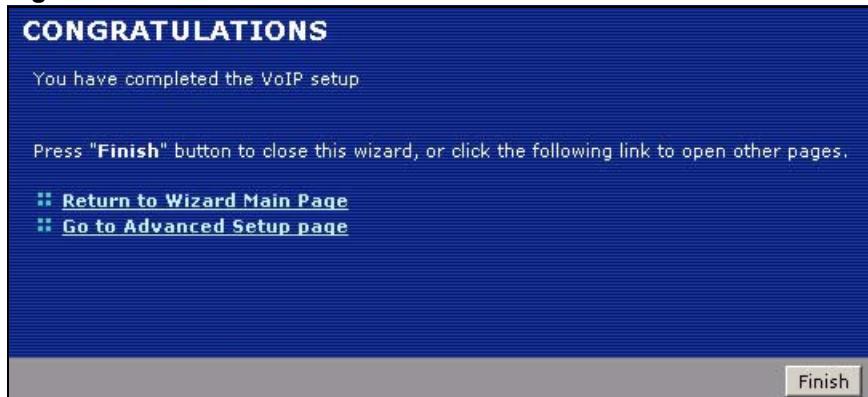
- When the SIP registration test screen displays, your ZyXEL Device attempts to register your SIP account with your VoIP service provider. Wait until it finishes.

**Figure 36** SIP Registration Test

- 6 The following screen displays if SIP account registration fails. Check whether you can access the Internet. If you have a successful Internet connection, click **Register Again**. Or click **Back** and check the information you entered in SIP account settings is correct. If you do not have a successful Internet connection, see [Chapter 28 on page 401](#) for troubleshooting.

**Figure 37** VoIP Wizard Fail

- 7 The congratulations screen displays if your SIP account registration was successful. You are ready to make and receive VoIP phone calls. Click **Return to Wizard Main Page** if you want to use another configuration wizard. Click **Go to Advanced Setup page** or **Finish** to close the wizard and go to the main web configurator screens.

**Figure 38** VoIP Wizard Finish

- 8 To call other VoIP users, you need to have their SIP numbers and ensure that their SIP accounts are registered and active. You can use your VoIP service provider's dialing plan to call SIP numbers.

You can also use your VoIP service provider's dialing plan to call regular phone numbers. You dial a prefix number, provided to you by your VoIP service provider, followed by a regular phone number.



---

To find out more information about configuring your VoIP features and making non-VoIP calls see [Chapter 11 on page 169](#).

---

# Bandwidth Management Wizard

This chapter shows you how to configure basic bandwidth management using the wizard screens.

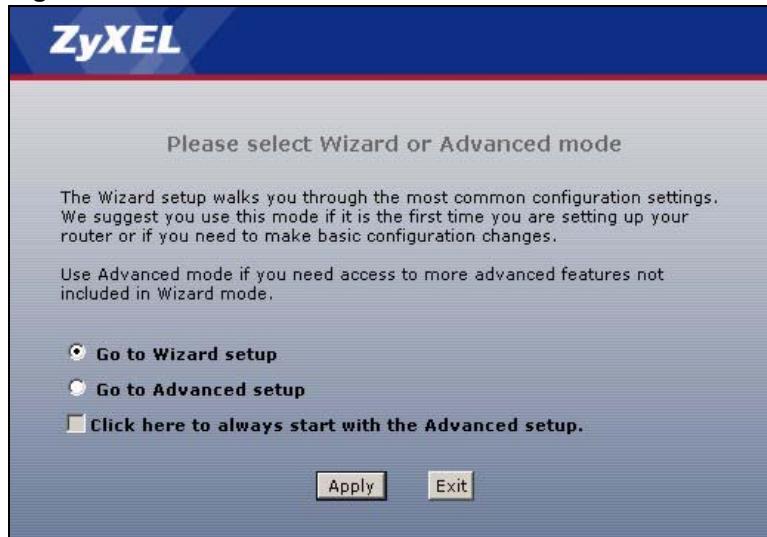
## 5.1 Introduction

Bandwidth management allows you to control the amount of bandwidth going out through the ZyXEL Device's WAN port and prioritize the distribution of the bandwidth according to service bandwidth requirements. This helps keep one service from using all of the available bandwidth and shutting out other users.

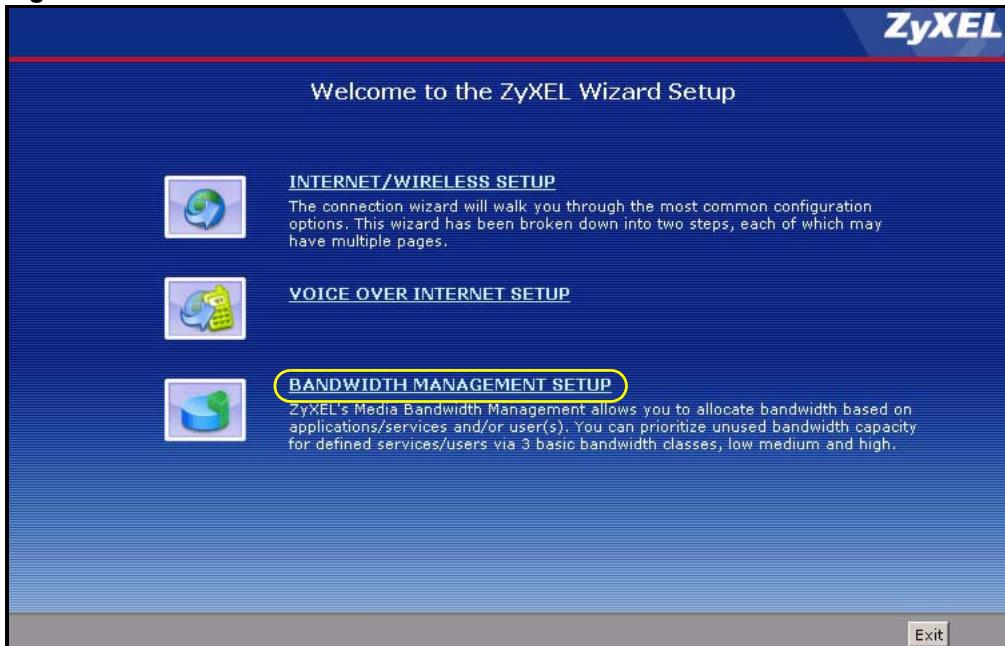
## 5.2 Bandwidth Management Wizard Setup

- 1 After you enter the password to access the web configurator, select **Go to Wizard setup** and click **Apply**. Otherwise, click the wizard icon (  ) in the top right corner of the web configurator to display the wizard main screen.

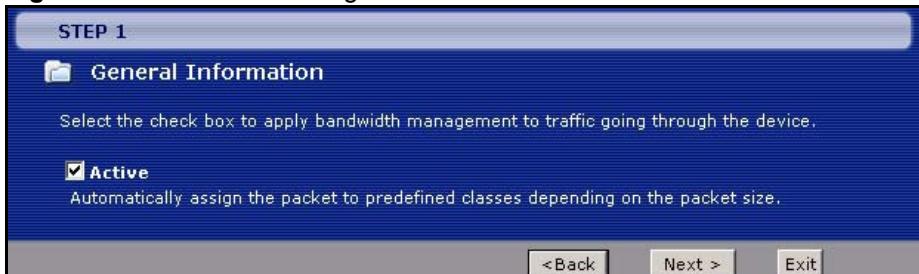
**Figure 39** Select a Mode



- 2 Click **BANDWIDTH MANAGEMENT SETUP**.

**Figure 40** Wizard: Welcome

- 3 Select **Active** to allocate bandwidth to packets based on the packet size.

**Figure 41** Bandwidth Management Wizard: General Information

The following fields describe the label in this screen.

**Table 16** Bandwidth Management Wizard: General Information

LABEL	DESCRIPTION
Active	Select the <b>Active</b> check box to have the ZyXEL Device apply bandwidth management to traffic going out through the ZyXEL Device's WAN, LAN or WLAN port based on the packet size.
Back	Click <b>Back</b> to display the previous screen.
Next	Click <b>Next</b> to proceed to the next screen.
Exit	Click <b>Exit</b> to close the wizard screen without saving.

- 4 Follow the on-screen instructions and click **Finish** to complete the wizard setup and save your configuration.

**Figure 42** Bandwidth Management Wizard: Complete





# Status Screens

Use the **Status** screens to look at the current status of the device, system resources, interfaces (LAN and WAN), and SIP accounts. You can also register and unregister SIP accounts. The **Status** screen also provides detailed information from Any IP and DHCP and statistics from VoIP, bandwidth management, and traffic.

## 6.1 Status Screen

Click **Status** to open this screen.

**Figure 43** Status Screen

Each field is described in the following table.

**Table 17** Status Screen

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want the ZyXEL Device to update this screen.
Apply	Click this to update this screen immediately.
Device Information	
Host Name	This field displays the ZyXEL Device system name. It is used for identification. You can change this in the <b>Maintenance &gt; System &gt; General</b> screen's <b>System Name</b> field.
Model Number	This is the model name of your device.

**Table 17** Status Screen

LABEL	DESCRIPTION
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your ZyXEL Device.
ZyNOS Firmware Version	This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. Click this to go to the screen where you can change it.
DSL Firmware Version	This field displays the current version of the device's DSL modem code.
WAN Information	
DSL Mode	This is the DSL standard that your ZyXEL Device is using.
IP Address	This field displays the current IP address of the ZyXEL Device in the WAN. Click this to go to the screen where you can change it.
IP Subnet Mask	This field displays the current subnet mask in the WAN.
Default Gateway	This is the IP address of the default gateway, if applicable.
VPI/VCI	This is the Virtual Path Identifier and Virtual Channel Identifier that you entered in the wizard or <b>WAN</b> screen.
LAN Information	
IP Address	This field displays the current IP address of the ZyXEL Device in the LAN. Click this to go to the screen where you can change it.
IP Subnet Mask	This field displays the current subnet mask in the LAN.
DHCP	This field displays what DHCP services the ZyXEL Device is providing to the LAN. Choices are: <b>Server</b> - The ZyXEL Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. <b>Relay</b> - The ZyXEL Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. <b>None</b> - The ZyXEL Device is not providing any DHCP services to the LAN. Click this to go to the screen where you can change it.
WLAN Information	("W" models only)
SSID	This is the descriptive name used to identify the ZyXEL Device in the wireless LAN. Click this to go to the screen where you can change it.
Channel	This is the channel number used by the ZyXEL Device now.
Security	This displays the type of security mode the ZyXEL Device is using in the wireless LAN.
Security	
Firewall	This displays whether or not the ZyXEL Device's firewall is activated. Click this to go to the screen where you can change it.
Content Filter	This displays whether or not the ZyXEL Device's content filtering is activated. Click this to go to the screen where you can change it.
System Status	
System Uptime	This field displays how long the ZyXEL Device has been running since it last started up. The ZyXEL Device starts up when you plug it in, when you restart it ( <b>Maintenance &gt; Tools &gt; Restart</b> ), or when you reset it (see <a href="#">Section 1.6 on page 47</a> ).

**Table 17** Status Screen

LABEL	DESCRIPTION
Current Date/ Time	This field displays the current date and time in the ZyXEL Device. You can change this in <b>Maintenance &gt; System &gt; Time Setting</b> .
System Mode	This displays whether the ZyXEL Device is functioning as a router or a bridge.
CPU Usage	This field displays what percentage of the ZyXEL Device's processing ability is currently used. When this percentage is close to 100%, the ZyXEL Device is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management; see <a href="#">Chapter 21 on page 331</a> ).
Memory Usage	This field displays what percentage of the ZyXEL Device's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the ZyXEL Device is probably becoming unstable, and you should restart the device. See <a href="#">Section 29.6 on page 413</a> , or turn off the device (unplug the power) for a few seconds.
Interface Status	
Interface	This column displays each interface the ZyXEL Device has.
Status	This field indicates whether or not the ZyXEL Device is using the interface. For the DSL interface, this field displays <b>Down</b> (line is down), <b>Up</b> (line is up or connected) if you're using Ethernet encapsulation and <b>Down</b> (line is down), <b>Up</b> (line is up or connected), <b>Idle</b> (line (ppp) idle), <b>Dial</b> (starting to trigger a call) and <b>Drop</b> (dropping a call) if you're using PPPoE encapsulation. For the LAN interface, this field displays <b>Up</b> when the ZyXEL Device is using the interface and <b>Down</b> when the ZyXEL Device is not using the interface. For the WLAN interface, it displays <b>Active</b> when WLAN is enabled or <b>Inactive</b> when WLAN is disabled.
Rate	For the LAN interface, this displays the port speed and duplex setting. For the DSL interface, it displays the downstream and upstream transmission rate. For the WLAN interface, it displays the transmission rate when WLAN is enabled or <b>N/A</b> when WLAN is disabled.
Summary	
Client List	Click this link to view current DHCP client information. See <a href="#">Section 8.6 on page 125</a> .
AnyIP Table	Click this link to view a list of IP addresses and MAC addresses of computers, which are not in the same subnet as the ZyXEL Device. See <a href="#">Section 6.2 on page 91</a> .
WLAN Status	Click this link to display the MAC address(es) of the wireless stations that are currently associating with the ZyXEL Device. See <a href="#">Section 6.3 on page 92</a> .
Bandwidth Status	Click this link to view the ZyXEL Device's bandwidth usage and allotments. See <a href="#">Section 21.8 on page 337</a> .
VPN Status	Click this link to view the ZyXEL Device's current VPN connections. See <a href="#">Section 18.16 on page 295</a> .
Packet Statistics	Click this link to view port status and packet specific statistics. See <a href="#">Section 6.4 on page 92</a> .
VoIP Statistics	Click this link to view statistics about your VoIP usage. See <a href="#">Section 6.5 on page 94</a> .
LED Status	Click this link to view the ZyXEL Device's port status. See <a href="#">Section 6.5 on page 94</a> .
VoIP Status	
Account	This column displays each SIP account in the ZyXEL Device.

**Table 17** Status Screen

LABEL	DESCRIPTION
Registration	<p>This field displays the current registration status of the SIP account. You have to register SIP accounts with a SIP server to use VoIP.</p> <p>If the SIP account is already registered with the SIP server,</p> <ul style="list-style-type: none"> <li>Click <b>Unregister</b> to delete the SIP account's registration in the SIP server. This does not cancel your SIP account, but it deletes the mapping between your SIP identity and your IP address or domain name.</li> <li>The second field displays <b>Registered</b>.</li> </ul> <p>If the SIP account is not registered with the SIP server,</p> <ul style="list-style-type: none"> <li>Click <b>Register</b> to have the ZyXEL Device attempt to register the SIP account with the SIP server.</li> <li>The second field displays the reason the account is not registered.</li> </ul> <p><b>Inactive</b> - The SIP account is not active. You can activate it in <b>VoIP &gt; SIP &gt; SIP Settings</b>.</p> <p><b>Register Fail</b> - The last time the ZyXEL Device tried to register the SIP account with the SIP server, the attempt failed. The ZyXEL Device automatically tries to register the SIP account when you turn on the ZyXEL Device or when you activate it.</p>
URI	This field displays the account number and service domain of the SIP account. You can change these in <b>VoIP &gt; SIP &gt; SIP Settings</b> .

## 6.2 Any IP Table

Click **Status > AnyIP Table** to access this screen. Use this screen to view the IP address and MAC address of each computer that is using the ZyXEL Device but is in a different subnet than the ZyXEL Device.

**Figure 44** Any IP Table

AnyIP Table		
#	IP Address	MAC Address
.....		
		<b>Refresh</b>

Each field is described in the following table.

**Table 18** Any IP Table

LABEL	DESCRIPTION
#	This field is a sequential value. It is not associated with a specific entry.
IP Address	This field displays the IP address of each computer that is using the ZyXEL Device but is in a different subnet than the ZyXEL Device.
MAC Address	This field displays the MAC address of the computer that is using the ZyXEL Device but is in a different subnet than the ZyXEL Device.
Refresh	Click this to update this screen.

## 6.3 WLAN Status

Click **Status > WLAN Status** to access this screen. Use this screen to view the wireless stations that are currently associated to the ZyXEL Device.

**Figure 45** WLAN Status

Wireless LAN- Association List		
#	MAC Address	Association Time
1	00:ac:c5:01:23:45	1
*****		
Refresh		

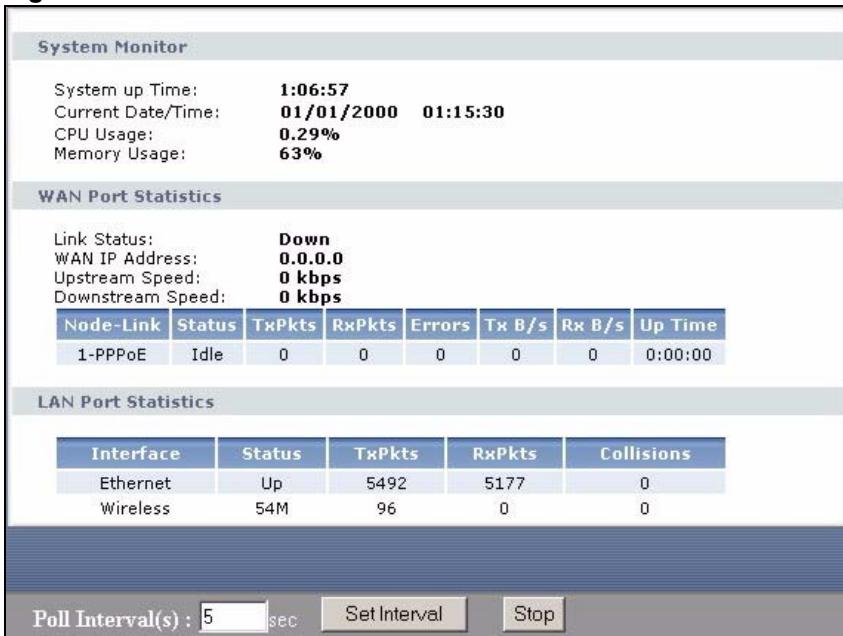
The following table describes the labels in this screen.

**Table 19** WLAN Status

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC (Media Access Control) address of an associated wireless station.
Association Time	This field displays the time a wireless station first associated with the ZyXEL Device.
Refresh	Click <b>Refresh</b> to reload this screen.

## 6.4 Packet Statistics

Click **Status > Packet Statistics** to access this screen. Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable.

**Figure 46** Packet Statistics

The following table describes the fields in this screen.

**Table 20** Packet Statistics

LABEL	DESCRIPTION
System Monitor	
System up Time	This is the elapsed time the system has been up.
Current Date/Time	This field displays your ZyXEL Device's present date and time.
CPU Usage	This field specifies the percentage of CPU utilization.
Memory Usage	This field specifies the percentage of memory utilization.
WAN Port Statistics	
Link Status	This is the status of your WAN link.
WAN IP Address	This is the IP address of the ZyXEL Device's WAN port.
Upstream Speed	This is the upstream speed of your ZyXEL Device.
Downstream Speed	This is the downstream speed of your ZyXEL Device.
Node-Link	This field displays the remote node index number and link type. Link types are PPPoA, ENET, RFC 1483 and PPPoE.
Status	This field displays <b>Down</b> (line is down), <b>Up</b> (line is up or connected) if you're using Ethernet encapsulation and <b>Down</b> (line is down), <b>Up</b> (line is up or connected), <b>Idle</b> (line (ppp) idle), <b>Dial</b> (starting to trigger a call) and <b>Drop</b> (dropping a call) if you're using PPPoE encapsulation.
TxPkts	This field displays the number of packets transmitted on this port.
RxPkts	This field displays the number of packets received on this port.
Errors	This field displays the number of error packets on this port.
Tx B/s	This field displays the number of bytes transmitted in the last second.
Rx B/s	This field displays the number of bytes received in the last second.
Up Time	This field displays the elapsed time this port has been up.
LAN Port Statistics	

**Table 20** Packet Statistics (continued)

LABEL	DESCRIPTION
Interface	This field displays either <b>Ethernet</b> (LAN ports) or <b>Wireless</b> (WLAN port).
Status	For the LAN ports, this field displays <b>Down</b> (line is down) or <b>Up</b> (line is up or connected). For the WLAN port, it displays the transmission rate when WLAN is enabled or <b>N/A</b> when WLAN is disabled.
TxPkts	This field displays the number of packets transmitted on this interface.
RxPkts	This field displays the number of packets received on this interface.
Collisions	This is the number of collisions on this interfaces.
Poll Interval(s)	Type the time interval for the browser to refresh system statistics.
Set Interval	Click this to apply the new poll interval you entered in the <b>Poll Interval</b> field above.
Stop	Click this button to halt the refreshing of the system statistics.

## 6.5 VoIP Statistics

Click **Status > VoIP Statistics** to access this screen.

**Figure 47** VoIP Statistics

The screenshot shows the VoIP Statistics screen with two main tables:

**SIP Status:**

Account	Registration	Last Registration	URI	Protocol	Message Waiting	Last Incoming Number	Last Outgoing Number
SIP1	Register Fail	N/A		UDP	No	N/A	N/A
SIP2	Inactive	N/A		UDP	No	N/A	N/A
SIP3	Inactive	N/A		UDP	No	N/A	N/A
SIP4	Inactive	N/A		UDP	No	N/A	N/A
SIP5	Inactive	N/A		UDP	No	N/A	N/A
SIP6	Inactive	N/A		UDP	No	N/A	N/A
SIP7	Inactive	N/A		UDP	No	N/A	N/A
SIP8	Inactive	N/A		UDP	No	N/A	N/A
SIP9	Inactive	N/A		UDP	No	N/A	N/A
SIP10	Inactive	N/A		UDP	No	N/A	N/A

**Call Statistics:**

Phone	Hook	Status	Codec	Peer Number	Duration	TxPkts	RxPkts	Tx B/s	Rx B/s
Phone1	On	N/A	N/A	N/A	0:00:00	0	0	0	0
Phone2	On	N/A	N/A	N/A	0:00:00	0	0	0	0

Poll Interval(s) :  sec

Each field is described in the following table.

**Table 21** VoIP Statistics

LABEL	DESCRIPTION
SIP Status	
Account	This column displays each SIP account in the ZyXEL Device.

**Table 21** VoIP Statistics

LABEL	DESCRIPTION
Registration	This field displays the current registration status of the SIP account. You can change this in the <b>Status</b> screen. <b>Registered</b> - The SIP account is registered with a SIP server. <b>Register Fail</b> - The last time the ZyXEL Device tried to register the SIP account with the SIP server, the attempt failed. The ZyXEL Device automatically tries to register the SIP account when you turn on the ZyXEL Device or when you activate it. <b>Inactive</b> - The SIP account is not active. You can activate it in <b>VoIP &gt; SIP &gt; SIP Settings</b> .
Last Registration	This field displays the last time you successfully registered the SIP account. It displays <b>N/A</b> if you never successfully registered this account.
URI	This field displays the account number and service domain of the SIP account. You can change these in <b>VoIP &gt; SIP &gt; SIP Settings</b> .
Protocol	This field displays the transport protocol the SIP account uses. SIP accounts always use UDP.
Message Waiting	This field indicates whether or not there are any messages waiting for the SIP account.
Last Incoming Number	This field displays the last number that called the SIP account. It displays <b>N/A</b> if no number has ever dialed the SIP account.
Last Outgoing Number	This field displays the last number the SIP account called. It displays <b>N/A</b> if the SIP account has never dialed a number.
Call Statistics	
Phone	This field displays each phone port in the ZyXEL Device.
Hook	This field indicates whether the phone is on the hook or off the hook. <b>On</b> - The phone is hanging up or already hung up. <b>Off</b> - The phone is dialing, calling, or connected.
Status	This field displays the current state of the phone call. <b>N/A</b> - There are no current VoIP calls, incoming calls or outgoing calls being made. <b>DIAL</b> - The callee's phone is ringing. <b>RING</b> - The phone is ringing for an incoming VoIP call. <b>Process</b> - There is a VoIP call in progress. <b>DISC</b> - The callee's line is busy, the callee hung up or your phone was left off the hook.
Codec	This field displays what voice codec is being used for a current VoIP call through a phone port.
Peer Number	This field displays the SIP number of the party that is currently engaged in a VoIP call through a phone port.
Duration	This field displays how long the current call has lasted.
Tx Pkts	This field displays the number of packets the ZyXEL Device has transmitted in the current call.
Rx Pkts	This field displays the number of packets the ZyXEL Device has received in the current call.
Tx B/s	This field displays how quickly the ZyXEL Device has transmitted packets in the current call. The rate is the average number of bytes transmitted per second.
Rx B/s	This field displays how quickly the ZyXEL Device has received packets in the current call. The rate is the average number of bytes transmitted per second.

**Table 21** VoIP Statistics

LABEL	DESCRIPTION
Poll Interval(s)	Enter how often you want the ZyXEL Device to update this screen, and click <b>Set Interval</b> .
Set Interval	Click this to make the ZyXEL Device update the screen based on the amount of time you specified in <b>Poll Interval</b> .
Stop	Click this to make the ZyXEL Device stop updating the screen.

## 6.6 LED Status

Use this screen to view the current status of each of the ZyXEL Device's ports. Click **Status > LED Status** to access this screen.

**Figure 48** LED Status

Each field is described in the following table.

**Table 22** LED Status

LABEL	STATUS	DESCRIPTION
Connection		
DSL	Green	The DSL port has a successful connection. The current downstream and upstream transmission rates display.
	Off	When the DSL port does not have a successful connection, it displays <b>Down</b> .
WLAN	Green	The wireless LAN is enabled. Your ZyXEL Device's SSID (Service Set IDentity) displays.
	Off	When the wireless LAN is disabled, it displays <b>Inactive</b> .
LAN 1~4	Green	The corresponding LAN port has a successful Ethernet connection.
	Off	The corresponding LAN port does not have a successful Ethernet connection.
Internet and Telephone		

**Table 22** LED Status

LABEL	STATUS	DESCRIPTION
Internet	Green	The ZyXEL Device has a successful Internet connection. This field displays the current IP address of the ZyXEL Device in the WAN.
	Off	The ZyXEL Device does not have a successful Internet connection. This field displays the default IP address of the ZyXEL Device in the WAN.
Phone 1 Phone 2	Green	This phone port has a successful SIP account registration. This field displays the number of the SIP account used to make outgoing calls on the corresponding phone port. This field also displays the current SIP registration status of the phone port. <b>On Register</b> - The phone port has a successful SIP account registration, and the phone connecting to this phone port is ready to make outgoing VoIP calls.
	Off	This phone port does not have a successful SIP account registration. This field displays the number of the SIP account used to make outgoing calls on the corresponding phone port. This field also displays the current SIP registration status. <b>Not Register</b> - The phone port has not registered a SIP account yet. <b>Register Fail</b> - The phone port tried to register a SIP account and the registration failed. <b>Inactive</b> - The phone port does not have a SIP account enabled. If you did not change the SIP account settings from the defaults, <b>ChangeMe</b> displays instead of the SIP account number.
Poll Interval (s)		Enter how often you want the ZyXEL Device to update this screen, and click <b>Set Interval</b> .
Set Interval		Click this to make the ZyXEL Device update the screen based on the amount of time you specified in <b>Poll Interval</b> .
Stop		Click this to make the ZyXEL Device stop updating the screen.



---

# PART III

# Network

---

- WAN Setup (101)
- LAN Setup (117)
- Wireless LAN (129)
- Network Address Translation (NAT) Screens (155)



# WAN Setup

This chapter describes how to configure WAN settings.

## 7.1 WAN Overview

A WAN (Wide Area Network) is an outside connection to another network or the Internet.

### 7.1.1 Encapsulation

Be sure to use the encapsulation method required by your ISP. The ZyXEL Device supports the following methods.

#### 7.1.1.1 ENET ENCAP

The MAC Encapsulated Routing Link Protocol (ENET ENCAP) is only implemented with the IP network protocol. IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged ATM cells. ENET ENCAP requires that you specify a gateway IP address in the **ENET ENCAP Gateway** field in the second wizard screen. You can get this information from your ISP.

#### 7.1.1.2 PPP over Ethernet

The ZyXEL Device supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPPoE** option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the ZyXEL Device (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the ZyXEL Device does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

#### 7.1.1.3 PPPoA

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). A PPPoA connection functions like a dial-up Internet connection. The ZyXEL Device encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider's (ISP) DSLAM (Digital Subscriber Line (DSL) Access Multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

#### 7.1.1.4 RFC 1483

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to RFC 1483 for more detailed information.

### 7.1.2 Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

#### 7.1.2.1 VC-based Multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

#### 7.1.2.2 LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

### 7.1.3 VPI and VCI

Be sure to use the correct Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers assigned to you. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Please see the appendix for more information.

### 7.1.4 IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address and ENET ENCAP gateway.

#### 7.1.4.1 IP Assignment with PPPoA or PPPoE Encapsulation

If you have a dynamic IP, then the **IP Address** and **ENET ENCAP Gateway** fields are not applicable (N/A). If you have a static IP, then you *only* need to fill in the **IP Address** field and *not* the **ENET ENCAP Gateway** field.

#### 7.1.4.2 IP Assignment with RFC 1483 Encapsulation

In this case the IP Address Assignment *must* be static with the same requirements for the **IP Address** and **ENET ENCAP Gateway** fields as stated above.

#### 7.1.4.3 IP Assignment with ENET ENCAP Encapsulation

In this case you can have either a static or dynamic IP. For a static IP you must fill in all the **IP Address** and **ENET ENCAP Gateway** fields as supplied by your ISP. However for a dynamic IP, the ZyXEL Device acts as a DHCP client on the WAN port and so the **IP Address** and **ENET ENCAP Gateway** fields are not applicable (N/A) as the DHCP server assigns them to the ZyXEL Device.

### 7.1.5 Nailed-Up Connection (PPP)

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The ZyXEL Device does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the ZyXEL Device will try to bring up the connection when turned on and whenever the connection is down. A nailed-up connection can be very expensive for obvious reasons.

Do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern.

### 7.1.6 NAT

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

## 7.2 Metric

The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".

The metric sets the priority for the ZyXEL Device's routes to the Internet. If any two of the default routes have the same metric, the ZyXEL Device uses the following pre-defined priorities:

- Normal route: designated by the ISP (see [Section 7.5 on page 106](#))
- Traffic-redirect route (see [Section 7.9 on page 114](#))
- WAN-backup route, also called dial-backup (see [Section 7.10 on page 114](#))

For example, if the normal route has a metric of "1" and the traffic-redirect route has a metric of "2" and dial-backup route has a metric of "3", then the normal route acts as the primary default route. If the normal route fails to connect to the Internet, the ZyXEL Device tries the traffic-redirect route next. In the same manner, the ZyXEL Device uses the dial-backup route if the traffic-redirect route also fails.

If you want the dial-backup route to take first priority over the traffic-redirect route or even the normal route, all you need to do is set the dial-backup route's metric to "1" and the others to "2" (or greater).

IP Policy Routing overrides the default routing behavior and takes priority over all of the routes mentioned above.

## 7.3 Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

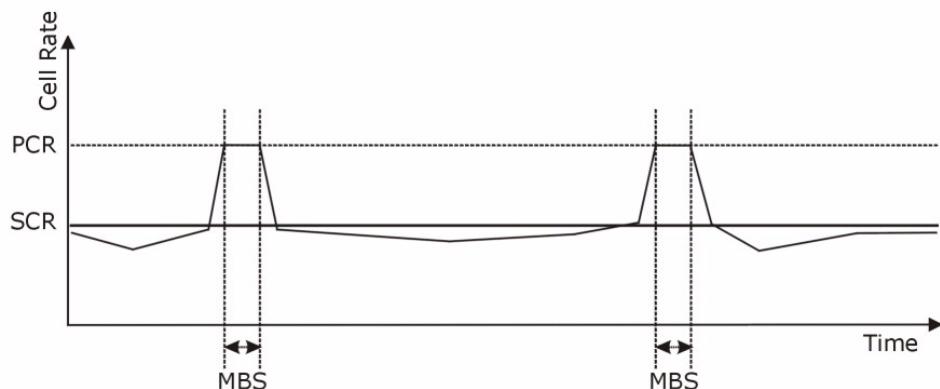
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

If the PCR, SCR or MBS is set to the default of "0", the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

**Figure 49** Example of Traffic Shaping



### 7.3.1 ATM Traffic Classes

These are the basic ATM traffic classes defined by the ATM Forum Traffic Management 4.0 Specification.

#### 7.3.1.1 Constant Bit Rate (CBR)

Constant Bit Rate (CBR) provides fixed bandwidth that is always available even if no data is being sent. CBR traffic is generally time-sensitive (doesn't tolerate delay). CBR is used for connections that continuously require a specific amount of bandwidth. A PCR is specified and if traffic exceeds this rate, cells may be dropped. Examples of connections that need CBR would be high-resolution video and voice.

#### 7.3.1.2 Variable Bit Rate (VBR)

The Variable Bit Rate (VBR) ATM traffic class is used with bursty connections. Connections that use the Variable Bit Rate (VBR) traffic class can be grouped into real time (VBR-RT) or non-real time (VBR-nRT) connections.

The VBR-RT (real-time Variable Bit Rate) type is used with bursty connections that require closely controlled delay and delay variation. It also provides a fixed amount of bandwidth (a PCR is specified) but is only available when data is being sent. An example of an VBR-RT connection would be video conferencing. Video conferencing requires real-time data transfers and the bandwidth requirement varies in proportion to the video image's changing dynamics.

The VBR-nRT (non real-time Variable Bit Rate) type is used with bursty connections that do not require closely controlled delay and delay variation. It is commonly used for "bursty" traffic typical on LANs. PCR and MBS define the burst levels, SCR defines the minimum level. An example of an VBR-nRT connection would be non-time sensitive data file transfers.

#### 7.3.1.3 Unspecified Bit Rate (UBR)

The Unspecified Bit Rate (UBR) ATM traffic class is for bursty data transfers. However, UBR doesn't guarantee any bandwidth and only delivers traffic when the network has spare bandwidth. An example application is background file transfer.

## 7.4 Zero Configuration Internet Access

Once you turn on and connect the ZyXEL Device to a telephone jack, it automatically detects the Internet connection settings (such as the VCI/VPI numbers and the encapsulation method) from the ISP and makes the necessary configuration changes. In cases where additional account information (such as an Internet account user name and password) is required or the ZyXEL Device cannot connect to the ISP, you will be redirected to web screen(s) for information input or troubleshooting.

Zero configuration for Internet access is disabled when

- the ZyXEL Device is in bridge mode
- you set the ZyXEL Device to use a static (fixed) WAN IP address.

## 7.5 Internet Access Setup

Use this screen to change your ZyXEL Device's WAN remote node settings. Click **Network > WAN > Internet Access Setup**. The screen differs by the encapsulation you select.

See [Section 7.1 on page 101](#) for more information.

**Figure 50** Internet Access Setup (PPPoE)

The following table describes the labels in this screen.

**Table 23** Internet Access Setup

LABEL	DESCRIPTION
General	
Mode	Select <b>Routing</b> (default) from the drop-down list box if your ISP allows multiple computers to share an Internet account. Otherwise select <b>Bridge</b> .
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the <b>Mode</b> field. If you select <b>Bridge</b> in the <b>Mode</b> field, select either <b>PPPoA</b> or <b>RFC 1483</b> . If you select <b>Routing</b> in the <b>Mode</b> field, select <b>PPPoA</b> , <b>RFC 1483</b> , <b>ENET ENCAP</b> or <b>PPPoE</b> .
User Name	(PPPoA and PPPoE encapsulation only) Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	(PPPoA and PPPoE encapsulation only) Enter the password associated with the user name above.
Service Name	(PPPoE only) Type the name of your PPPoE service here.

**Table 23** Internet Access Setup (continued)

LABEL	DESCRIPTION
Multiplexing	Select the method of multiplexing used by your ISP from the drop-down list. Choices are <b>VC</b> or <b>LLC</b> .
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
IP Address	
IP Address	This option is available if you select <b>Routing</b> in the <b>Mode</b> field. A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select <b>Obtain an IP Address Automatically</b> if you have a dynamic IP address; otherwise select <b>Static IP Address</b> and type your ISP assigned IP address in the <b>IP Address</b> field below.
Subnet Mask (ENET ENCAP encapsulation only)	Enter a subnet mask in dotted decimal notation. Refer to the appendix to calculate a subnet mask if you are implementing subnetting.
Gateway IP address (ENET ENCAP encapsulation only)	You must specify a gateway IP address (supplied by your ISP) when you select <b>ENET ENCAP</b> in the <b>Encapsulation</b> field
DNS Server	
First DNS Server Second DNS Server Third DNS Server	Select <b>Obtained From ISP</b> if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address). Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose <b>User-Defined</b> , but leave the IP address set to 0.0.0.0, <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b> . If you set a second choice to <b>User-Defined</b> , and enter the same IP address, the second <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b> . Select <b>DNS Relay</b> to have the ZyXEL Device act as a DNS proxy only when the ISP uses IPCP DNS server extensions. The ZyXEL Device's LAN IP address displays in the field to the right (read-only). The ZyXEL Device tells the DHCP clients on the LAN that the ZyXEL Device itself is the DNS server. When a computer on the LAN sends a DNS query to the ZyXEL Device, the ZyXEL Device forwards the query to the real DNS server learned through IPCP and relays the response back to the computer. You can only select <b>DNS Relay</b> for one of the three servers; if you select <b>DNS Relay</b> for a second or third DNS server, that choice changes to <b>None</b> after you click <b>Apply</b> . Select <b>None</b> if you do not want to configure DNS servers. You must have another DNS server on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Connection (PPPoA and PPPoE encapsulation only)	
Nailed-Up Connection	Select <b>Nailed-Up Connection</b> when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select <b>Connect on Demand</b> when you don't want the connection up all the time and specify an idle time-out in the <b>Max Idle Timeout</b> field.

**Table 23** Internet Access Setup (continued)

LABEL	DESCRIPTION
Max Idle Timeout	Specify an idle time-out in the <b>Max Idle Timeout</b> field when you select <b>Connect on Demand</b> . The default setting is 0, which means the Internet session will not timeout.
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Advanced Setup	Click this button to display the <b>Advanced WAN Setup</b> screen and edit more details of your WAN setup.

### 7.5.1 Advanced Internet Access Setup

Use this screen to edit your ZyXEL Device's advanced WAN settings. Click the **Advanced Setup** button in the **Internet Access Setup** screen. The screen appears as shown.

**Figure 51** Advanced Internet Access Setup

The following table describes the labels in this screen.

**Table 24** Advanced Internet Access Setup

LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. Use this field to control how much routing information the ZyXEL Device sends and receives on the subnet. Select the RIP direction from <b>None</b> , <b>Both</b> , <b>In Only</b> and <b>Out Only</b> .
RIP Version	Select the RIP version from <b>RIP-1</b> , <b>RIP-2B</b> and <b>RIP-2M</b> .
Multicast	Multicast packets are sent to a group of computers on the LAN and are an alternative to unicast packets (packets sent to one computer) and broadcast packets (packets sent to every computer). IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports both IGMP version 1 ( <b>IGMP-v1</b> ) and <b>IGMP-v2</b> . Select <b>None</b> to disable it.

**Table 24** Advanced Internet Access Setup (continued)

LABEL	DESCRIPTION
ATM QoS	
ATM QoS Type	Select <b>CBR</b> (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select <b>UBR</b> (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select <b>VBR-RT</b> (real-time Variable Bit Rate) type for applications with bursty connections that require closely controlled delay and delay variation. Select <b>VBR-nRT</b> (non real-time Variable Bit Rate) type for connections that do not require closely controlled delay and delay variation.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
Zero Configuration	This feature is not applicable/available when you configure the ZyXEL Device to use a static WAN IP address or in bridge mode. Select <b>Yes</b> to set the ZyXEL Device to automatically detect the Internet connection settings (such as the VCI/VPI numbers and the encapsulation method) from the ISP and make the necessary configuration changes. Select <b>No</b> to disable this feature. You must manually configure the ZyXEL Device for Internet access.
PPPoE Passthrough (PPPoE encapsulation only)	This field is available when you select <b>PPPoE</b> encapsulation. In addition to the ZyXEL Device's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the ZyXEL Device. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for application where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 7.6 WAN More Connections

The ZyXEL Device allows you to configure more than one Internet access connection. To configure additional Internet access connections click **Network > WAN > More Connections**. The screen differs by the encapsulation you select.

**Figure 52** WAN More Connections

		Internet Access Setup	More Connections	WAN Backup Setup	
#	Active	Name	VPI/VCI	Encapsulation	Modify
1	-	Internet Connection	0/33	PPPoE	 
2	-	--	--	--	 
3	-	--	--	--	 
4	-	--	--	--	 
5	-	--	--	--	 
6	-	--	--	--	 
7	-	--	--	--	 
8	-	--	--	--	 

**Apply**      **Cancel**

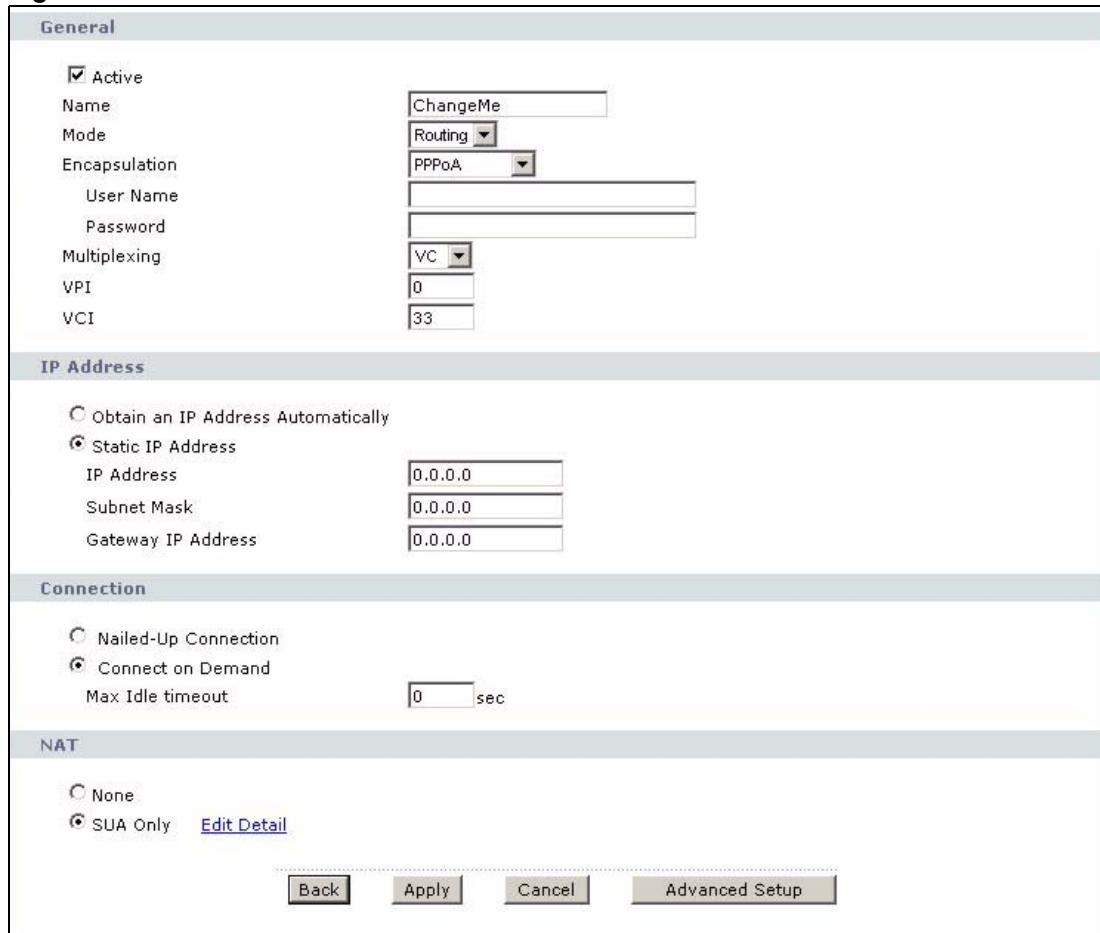
The following table describes the labels in this screen.

**Table 25** Advanced Internet Access Setup

LABEL	DESCRIPTION
#	This is an index number indicating the number of the corresponding connection.
Active	This field indicates whether the connection is active or not.
Name	This is the name you gave to the Internet connection.
VPI/VCI	This field displays the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers configured for this WAN connection.
Encapsulation	This field indicates the encapsulation method of the Internet connection.
Modify	Click the modify icon to edit the Internet connection settings. The fields Click this icon on an empty configuration to add a new Internet access setup. Click the delete icon to remove the Internet access setup from your connection list.
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 7.7 More Connections Edit

Click the edit icon in the **More Connections** screen to configure a node.

**Figure 53** More Connections Edit

The following table describes the labels in this screen.

**Table 26** More Connections Edit

LABEL	DESCRIPTION
General	
Active	Select the check box to activate or clear the check box to deactivate this node.
Name	Enter a unique, descriptive name of up to 20 characters for this node. You can use alphanumeric characters and the hyphen “-”, underscore “_” and @.
General	
Mode	Select <b>Routing</b> from the drop-down list box if your ISP allows multiple computers to share an Internet account. If you select <b>Bridge</b> , the ZyXEL Device will forward any packet that it does not route to this remote node; otherwise, the packets are discarded.
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices are <b>PPPoA</b> , <b>RFC 1483</b> , <b>ENET ENCAP</b> or <b>PPPoE</b> .
User Name	(PPPoA and PPPoE encapsulation only) Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	(PPPoA and PPPoE encapsulation only) Enter the password associated with the user name above.

**Table 26** More Connections Edit (continued)

LABEL	DESCRIPTION
Service Name	(PPPoE only) Type the name of your PPPoE service here.
Multiplexing	Select the method of multiplexing used by your ISP from the drop-down list. Choices are <b>VC</b> or <b>LLC</b> . By prior agreement, a protocol is assigned a specific virtual circuit, for example, VC1 will carry IP. If you select VC, specify separate VPI and VCI numbers for each protocol. For LLC-based multiplexing or PPP encapsulation, one VC carries multiple protocols with protocol identifying information being contained in each packet header. In this case, only one set of VPI and VCI numbers need be specified for all protocols.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
IP Address	This option is available if you select <b>Routing</b> in the <b>Mode</b> field. A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. If you use the encapsulation type except <b>RFC 1483</b> , select <b>Obtain an IP Address Automatically</b> when you have a dynamic IP address; otherwise select <b>Static IP Address</b> and type your ISP assigned IP address in the <b>IP Address</b> field below. If you use <b>RFC 1483</b> , enter the IP address given by your ISP in the <b>IP Address</b> field.
Subnet Mask	Enter a subnet mask in dotted decimal notation. Refer to the appendices to calculate a subnet mask if you are implementing subnetting.
Gateway IP address	Specify a gateway IP address (supplied by your ISP).
Connection	
Nailed-Up Connection	Select <b>Nailed-Up Connection</b> when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select <b>Connect on Demand</b> when you don't want the connection up all the time and specify an idle time-out in the <b>Max Idle Timeout</b> field.
Max Idle Timeout	Specify an idle time-out in the <b>Max Idle Timeout</b> field when you select <b>Connect on Demand</b> . The default setting is 0, which means the Internet session will not timeout.
NAT	<b>SUA only</b> and <b>Full Feature</b> are available only when you select <b>Routing</b> in the <b>Mode</b> field. Select <b>SUA Only</b> if you have one public IP address, <b>Full Feature</b> if you have multiple public IP addresses (for address translation) or <b>None</b> to disable NAT. When selecting <b>Full Feature</b> , configure address mapping sets in the <b>Address Mapping</b> screen. Select one of the NAT server sets (2-10) in the <b>Port Forwarding</b> screen (see <a href="#">Chapter 10 on page 155</a> for details) and type that number here.
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Advanced Setup	Click this button to edit RIP, multicast and ATM QoS settings.

## 7.8 More Connections Edit Advanced

Click the **Advanced** button in the **More Connections Edit** screen to display the following screen.

**Figure 54** More Connections Edit Advanced

The following table describes the labels in this screen.

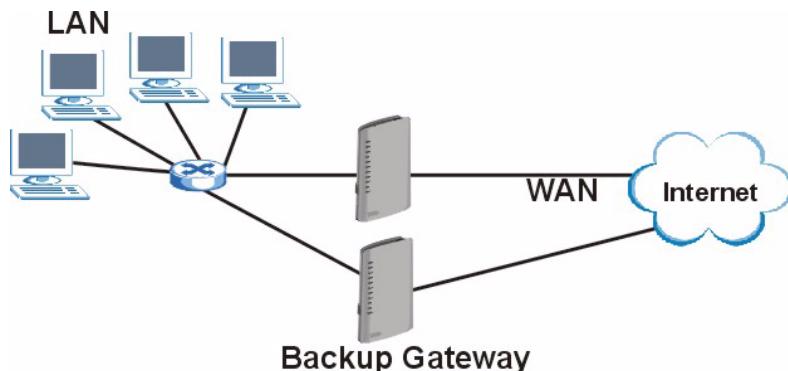
**Table 27** More Connections Edit Advanced

LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	Select the RIP direction from <b>None</b> , <b>Both</b> , <b>In Only</b> and <b>Out Only</b> .
RIP Version	Select the RIP version from <b>RIP-1</b> , <b>RIP-2B</b> and <b>RIP-2M</b> .
Multicast	IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports both IGMP version 1 ( <b>IGMP-v1</b> ) and <b>IGMP-v2</b> . Select <b>None</b> to disable it.
ATM QoS	
ATM QoS Type	Select <b>CBR</b> (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select <b>UBR</b> (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select <b>VBR</b> (Variable Bit Rate) for bursty traffic and bandwidth sharing with other applications.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 7.9 Traffic Redirect

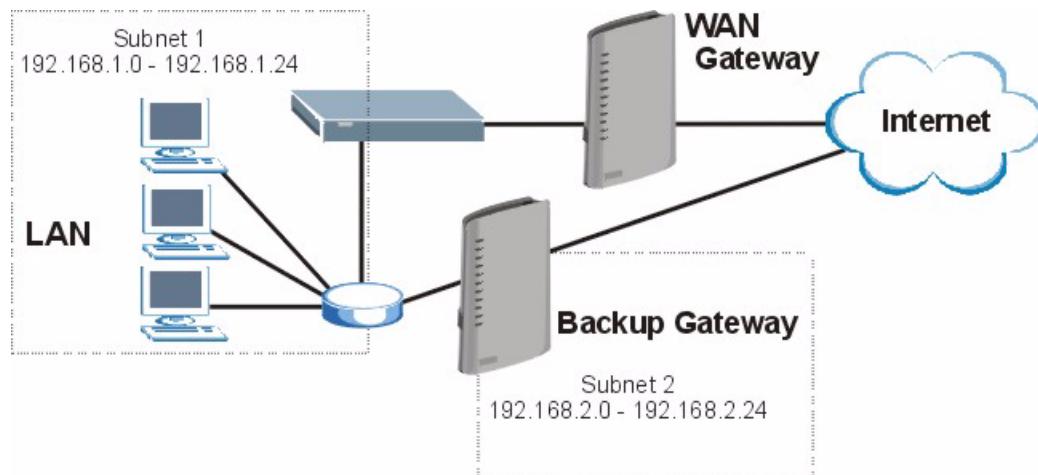
Traffic redirect forwards traffic to a backup gateway when the ZyXEL Device cannot connect to the Internet. An example is shown in the figure below.

**Figure 55** Traffic Redirect Example



The following network topology allows you to avoid triangle route security issues when the backup gateway is connected to the LAN. Use IP alias to configure the LAN into two or three logical networks with the ZyXEL Device itself as the gateway for each LAN network. Put the protected LAN in one subnet (Subnet 1 in the following figure) and the backup gateway in another subnet (Subnet 2). Configure filters that allow packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

**Figure 56** Traffic Redirect LAN Setup



## 7.10 WAN Backup Setup

Use this screen to configure your ZyXEL Device's WAN backup. Click **Network > WAN > WAN Backup Setup**.

**Figure 57** WAN Backup Setup

The screenshot shows the 'WAN Backup Setup' interface. At the top, there are tabs for 'Internet Access Setup', 'More Connections', and 'WAN Backup Setup'. The 'WAN Backup Setup' tab is selected. Below the tabs, there are two main sections: 'WAN Backup Setup' and 'Traffic Redirect'.

**WAN Backup Setup:**

- Backup Type:** A dropdown menu set to 'DSL Link'.
- Check WAN IP Address 1:** An input field containing '0.0.0.0'.
- Check WAN IP Address 2:** An input field containing '0.0.0.0'.
- Check WAN IP Address 3:** An input field containing '0.0.0.0'.
- Fail Tolerance:** An input field containing '0'.
- Recovery Interval:** An input field containing '0 sec'.
- Timeout:** An input field containing '0 sec'.

**Traffic Redirect:**

- Active Traffic Redirect:** A checkbox that is unchecked.
- Metric:** An input field containing '15'.
- Backup Gateway:** An input field containing '0.0.0.0'.

At the bottom right are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

**Table 28** WAN Backup Setup

LABEL	DESCRIPTION
Backup Type	Select the method that the ZyXEL Device uses to check the DSL connection. Select <b>DSL Link</b> to have the ZyXEL Device check if the connection to the DSLAM is up. Select <b>ICMP</b> to have the ZyXEL Device periodically ping the IP addresses configured in the <b>Check WAN IP Address</b> fields.
Check WAN IP Address1-3	<p>Configure this field to test your ZyXEL Device's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address).</p> <p><b>Note:</b> If you activate either traffic redirect or dial backup, you must configure at least one IP address here.</p> <p>When using a WAN backup connection, the ZyXEL Device periodically pings the addresses configured here and uses the other WAN backup connection (if configured) if there is no response.</p>
Fail Tolerance	Type the number of times (2 recommended) that your ZyXEL Device may ping the IP addresses configured in the <b>Check WAN IP Address</b> field without getting a response before switching to a WAN backup connection (or a different WAN backup connection).
Recovery Interval	<p>When the ZyXEL Device is using a lower priority connection (usually a WAN backup connection), it periodically checks whether or not it can use a higher priority connection.</p> <p>Type the number of seconds (30 recommended) for the ZyXEL Device to wait between checks. Allow more time if your destination IP address handles lots of traffic.</p>
Timeout	Type the number of seconds (3 recommended) for your ZyXEL Device to wait for a ping response from one of the IP addresses in the <b>Check WAN IP Address</b> field before timing out the request. The WAN connection is considered "down" after the ZyXEL Device times out the number of times specified in the <b>Fail Tolerance</b> field. Use a higher value in this field if your network is busy or congested.

**Table 28** WAN Backup Setup (continued)

LABEL	DESCRIPTION
Traffic Redirect	Traffic redirect forwards traffic to a backup gateway when the ZyXEL Device cannot connect to the Internet.
Active Traffic Redirect	Select this check box to have the ZyXEL Device use traffic redirect if the normal WAN connection goes down.  Note: If you activate traffic redirect, you must configure at least one Check WAN IP Address.
Metric	This field sets this route's priority among the routes the ZyXEL Device uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Backup Gateway	Type the IP address of your backup gateway in dotted decimal notation. The ZyXEL Device automatically forwards traffic to this IP address if the ZyXEL Device's Internet connection terminates.
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

# LAN Setup

This chapter describes how to configure LAN settings.

## 8.1 LAN Overview

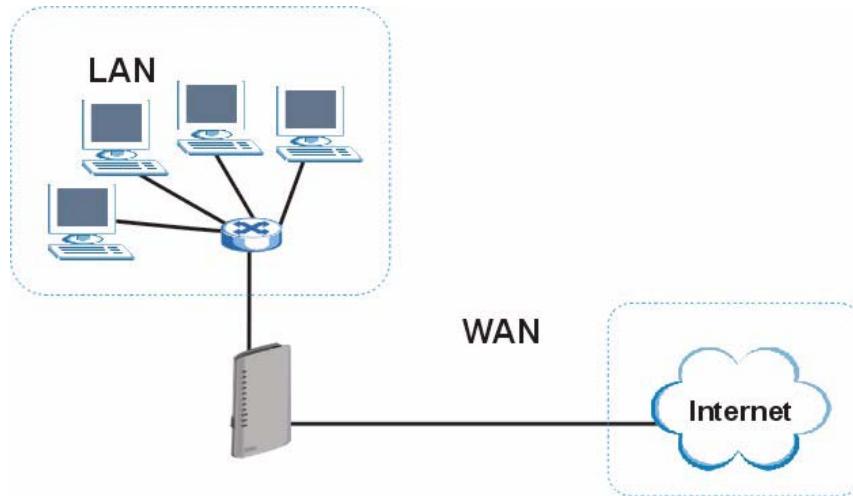
A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

See [Section 8.4 on page 122](#) for information on configuring the LAN screens.

### 8.1.1 LANs, WANs and the ZyXEL Device

The actual physical connection determines whether the ZyXEL Device ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

**Figure 58** LAN and WAN IP Addresses



## 8.1.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyXEL Device as a DHCP server or disable it. When configured as a server, the ZyXEL Device provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

### 8.1.2.1 IP Pool Setup

The ZyXEL Device is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

## 8.2 DNS Server Addresses

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the DNS Server fields in the **LAN Setup** screen.
- Some ISPs choose to disseminate the DNS server addresses using the DNS server extensions of IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The ZyXEL Device supports the IPCP DNS server extensions through the DNS proxy feature.

The ZyXEL Device acts as a DNS proxy when the **Primary** and **Secondary DNS Server** fields are left blank in the **LAN Setup** screen.

Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **LAN Setup** screen.

## 8.3 LAN TCP/IP

The ZyXEL Device has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

### 8.3.1 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the ZyXEL Device. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your ZyXEL Device, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

### 8.3.1.1 Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.



Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, "Address Allocation for Private Internets" and RFC 1466, "Guidelines for Management of IP Address Space".

---

### 8.3.2 RIP Setup

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. When set to:

- **Both** - the ZyXEL Device will broadcast its routing table periodically and incorporate the RIP information that it receives.
- **In Only** - the ZyXEL Device will not send any RIP packets but will accept all RIP packets received.
- **Out Only** - the ZyXEL Device will send out RIP packets but will not accept any RIP packets received.
- **None** - the ZyXEL Device will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). RIP-1 is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both RIP-2B and RIP-2M sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting.

### 8.3.3 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The ZyXEL Device supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the ZyXEL Device queries all directly connected networks to gather group membership. After that, the ZyXEL Device periodically updates this information. IP multicasting can be enabled/disabled on the ZyXEL Device LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

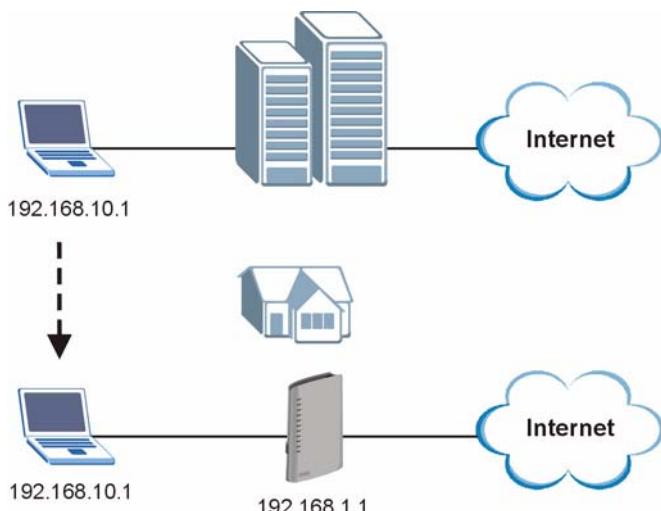
### 8.3.4 Any IP

Traditionally, you must set the IP addresses and the subnet masks of a computer and the ZyXEL Device to be in the same subnet to allow the computer to access the Internet (through the ZyXEL Device). In cases where your computer is required to use a static IP address in another network, you may need to manually configure the network settings of the computer every time you want to access the Internet via the ZyXEL Device.

With the Any IP feature and NAT enabled, the ZyXEL Device allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, when the IP addresses of the computer and the ZyXEL Device are not in the same subnet. Whether a computer is set to use a dynamic or static (fixed) IP address, you can simply connect the computer to the ZyXEL Device and access the Internet.

The following figure depicts a scenario where a computer is set to use a static private IP address in the corporate environment. In a residential house where a ZyXEL Device is installed, you can still use the computer to access the Internet without changing the network settings, even when the IP addresses of the computer and the ZyXEL Device are not in the same subnet.

**Figure 59** Any IP Example



The Any IP feature does not apply to a computer using either a dynamic IP address or a static IP address that is in the same subnet as the ZyXEL Device's IP address.



You must enable NAT/SUA to use the Any IP feature on the ZyXEL Device.

#### 8.3.4.1 How Any IP Works

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network. IP routing table is defined on IP Ethernet devices (the ZyXEL Device) to decide which hop to use, to help forward data along to its specified destination.

The following lists out the steps taken, when a computer tries to access the Internet for the first time through the ZyXEL Device.

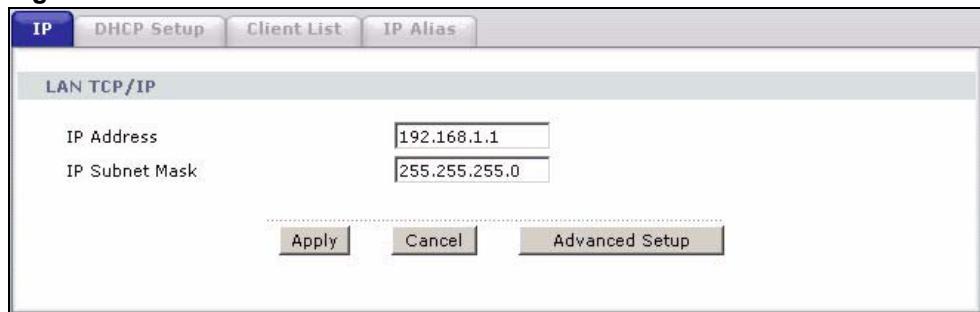
- 1 When a computer (which is in a different subnet) first attempts to access the Internet, it sends packets to its default gateway (which is not the ZyXEL Device) by looking at the MAC address in its ARP table.
- 2 When the computer cannot locate the default gateway, an ARP request is broadcast on the LAN.
- 3 The ZyXEL Device receives the ARP request and replies to the computer with its own MAC address.
- 4 The computer updates the MAC address for the default gateway to the ARP table. Once the ARP table is updated, the computer is able to access the Internet through the ZyXEL Device.
- 5 When the ZyXEL Device receives packets from the computer, it creates an entry in the IP routing table so it can properly forward packets intended for the computer.

After all the routing information is updated, the computer can access the ZyXEL Device and the Internet as if it is in the same subnet as the ZyXEL Device.

## 8.4 Configuring LAN IP

Click **Network > LAN** to open the **IP** screen. See [Section 8.1 on page 117](#) for background information. Use this screen to set the Local Area Network IP address and subnet mask of your ZyXEL Device.

**Figure 60** LAN IP



The following table describes the fields in this screen.

**Table 29** LAN IP

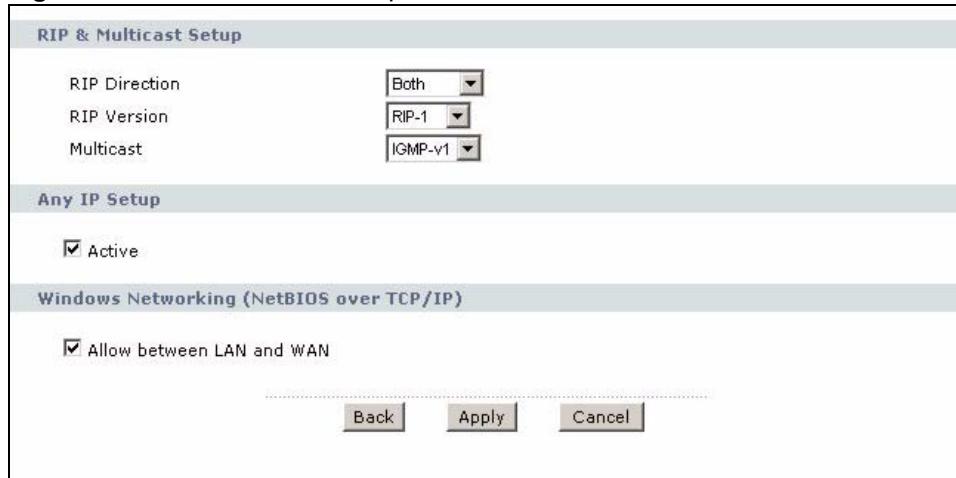
LABEL	DESCRIPTION
LAN TCP/IP	
IP Address	Enter the LAN IP address you want to assign to your ZyXEL Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
IP Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your ZyXEL Device automatically computes the subnet mask based on the IP Address you enter, so do not change this field unless you are instructed to do so.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.

**Table 29** LAN IP (continued)

LABEL	DESCRIPTION
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Advanced Setup	Click this button to display the <b>Advanced LAN Setup</b> screen and edit more details of your LAN setup.

### 8.4.1 Configuring Advanced LAN Setup

Use this screen to edit your ZyXEL Device's RIP, multicast, any IP and Windows Networking settings. Click the **Advanced Setup** button in the **LAN IP** screen. The screen appears as shown.

**Figure 61** Advanced LAN Setup

The following table describes the labels in this screen.

**Table 30** Advanced LAN Setup

LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	Select the RIP direction from <b>None</b> , <b>Both</b> , <b>In Only</b> and <b>Out Only</b> .
RIP Version	Select the RIP version from <b>RIP-1</b> , <b>RIP-2B</b> and <b>RIP-2M</b> .
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports both IGMP version 1 ( <b>IGMP-v1</b> ) and <b>IGMP-v2</b> . Select <b>None</b> to disable it.
Any IP Setup	Select the <b>Active</b> check box to enable the Any IP feature. This allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, even when the IP addresses of the computer and the ZyXEL Device are not in the same subnet. When you disable the Any IP feature, only computers with dynamic IP addresses or static IP addresses in the same subnet as the ZyXEL Device's LAN IP address can connect to the ZyXEL Device or access the Internet through the ZyXEL Device.
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.

**Table 30** Advanced LAN Setup (continued)

LABEL	DESCRIPTION
Allow between LAN and WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 8.5 DHCP Setup

Click **Network > DHCP Setup** to open this screen. Use this screen to configure the DNS server information that the ZyXEL Device sends to the DHCP client devices on the LAN.

**Figure 62** DHCP Setup

The screenshot shows the DHCP Setup interface. At the top, there are tabs for IP, DHCP Setup (which is selected), Client List, and IP Alias. The main area is titled "DHCP Setup". It contains fields for "DHCP" (set to "Server"), "IP Pool Starting Address" (192.168.1.33), "Pool Size" (32), and "Remote DHCP Server" (0.0.0.0). Below this is a section titled "DNS Server" with fields for "DNS Servers Assigned by DHCP Server". It lists three entries: "First DNS Server" (Obtained From ISP, 0.0.0.0), "Second DNS Server" (Obtained From ISP, 0.0.0.0), and "Third DNS Server" (Obtained From ISP, 0.0.0.0). At the bottom are "Apply" and "Cancel" buttons.

The following table describes the labels in this screen.

**Table 31** DHCP Setup

LABEL	DESCRIPTION
DHCP Setup	
DHCP	If set to <b>Server</b> , your ZyXEL Device can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. If set to <b>None</b> , the DHCP server will be disabled. If set to <b>Relay</b> , the ZyXEL Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the <b>Remote DHCP Server</b> field in this case. When DHCP is used, the following items need to be set:

**Table 31** DHCP Setup

LABEL	DESCRIPTION
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
Remote DHCP Server	If <b>Relay</b> is selected in the <b>DHCP</b> field above then enter the IP address of the actual remote DHCP server here.
DNS Server	
DNS Servers Assigned by DHCP Server	The ZyXEL Device passes a DNS (Domain Name System) server IP address to the DHCP clients.
First DNS Server Second DNS Server Third DNS Server	Select <b>Obtained From ISP</b> if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address). Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose <b>User-Defined</b> , but leave the IP address set to 0.0.0.0, <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b> . If you set a second choice to <b>User-Defined</b> , and enter the same IP address, the second <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b> . Select <b>DNS Relay</b> to have the ZyXEL Device act as a DNS proxy only when the ISP uses IPCP DNS server extensions. The ZyXEL Device's LAN IP address displays in the field to the right (read-only). The ZyXEL Device tells the DHCP clients on the LAN that the ZyXEL Device itself is the DNS server. When a computer on the LAN sends a DNS query to the ZyXEL Device, the ZyXEL Device forwards the query to the real DNS server learned through IPCP and relays the response back to the computer. You can only select <b>DNS Relay</b> for one of the three servers; if you select <b>DNS Relay</b> for a second or third DNS server, that choice changes to <b>None</b> after you click <b>Apply</b> . Select <b>None</b> if you do not want to configure DNS servers. You must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 8.6 LAN Client List

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

Click **Network > LAN > Client List** to open the following screen. Use this screen to change your ZyXEL Device's static DHCP settings.

**Figure 63** LAN Client List

IP	DHCP Setup	<b>Client List</b>	IP Alias
<b>DHCP Client Table</b>			
IP Address	192.168.1.66	MAC Address	AA:BB:CC:EE:EE:EE
		Add	
#	Status	Host Name	IP Address
1		IBM1	192.168.1.33
2			192.168.1.34
3		HP	192.168.1.99
			MAC Address
			AA:BB:CC:DD:EE:FF
			AA:BB:CC:KK:FF:GG
			Reserve
			<input checked="" type="checkbox"/>
			Modify
Apply		Reset	Refresh

The following table describes the labels in this screen.

**Table 32** LAN Client List

LABEL	DESCRIPTION
IP Address	Enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify.
MAC Address	Enter the MAC address of a computer on your LAN.
Add	Click <b>Add</b> to add a static DHCP entry.
#	This is the index number of the static IP table entry (row).
Status	This field displays whether the client is connected to the ZyXEL Device.
Host Name	This field displays the computer host name.
IP Address	This field displays the IP address relative to the # field listed above.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
Reserve	Select the check box in the heading row to automatically select all check boxes or select the check box(es) in each entry to have the ZyXEL Device always assign the selected entry(ies)'s IP address(es) to the corresponding MAC address(es) (and host name(s)). You can select up to 128 entries in this table. After you click <b>Apply</b> , the MAC address and IP address also display in the <b>LAN Static DHCP</b> screen (where you can edit them).
Modify	Click the modify icon to have the IP address field editable and change it.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Refresh	Click <b>Refresh</b> to reload the DHCP table.

## 8.7 LAN IP Alias

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyXEL Device supports three logical LAN interfaces via its single physical Ethernet interface with the ZyXEL Device itself as the gateway for each LAN network.

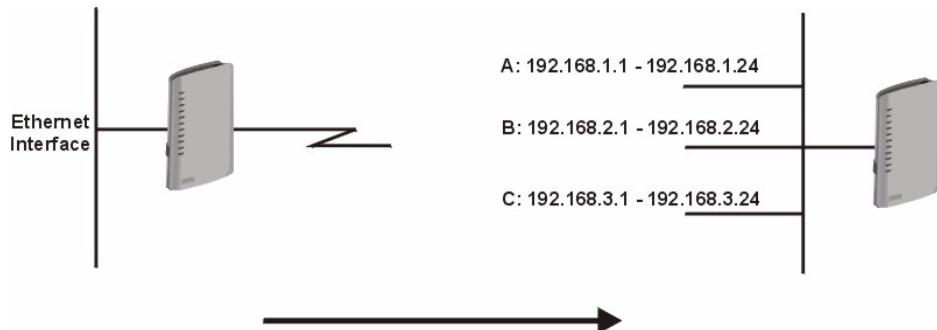
When you use IP alias, you can also configure firewall rules to control access between the LAN's logical networks (subnets).



Make sure that the subnets of the logical networks do not overlap.

The following figure shows a LAN divided into subnets A, B, and C.

**Figure 64** Physical Network & Partitioned Logical Networks



Click **Network > LAN > IP Alias** to open the following screen. Use this screen to change your ZyXEL Device's IP alias settings.

**Figure 65** LAN IP Alias

IP	DHCP Setup	Client List	IP Alias
<b>IP Alias 1</b> <input type="checkbox"/> IP Alias 1			
IP Address	0.0.0.0		
IP Subnet Mask	0.0.0.0		
RIP Direction	None		
RIP Version	N/A		
<b>IP Alias 2</b> <input type="checkbox"/> IP Alias 2			
IP Address	0.0.0.0		
IP Subnet Mask	0.0.0.0		
RIP Direction	None		
RIP Version	N/A		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

The following table describes the labels in this screen.

**Table 33** LAN IP Alias

LABEL	DESCRIPTION
IP Alias 1, 2	Select the check box to configure another LAN network for the ZyXEL Device.
IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address.
IP Subnet Mask	Your ZyXEL Device will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL Device.
RIP Direction	RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. The <b>RIP Direction</b> field controls the sending and receiving of RIP packets. Select the RIP direction from <b>Both/In Only/Out Only/None</b> . When set to <b>Both</b> or <b>Out Only</b> , the ZyXEL Device will broadcast its routing table periodically. When set to <b>Both</b> or <b>In Only</b> , it will incorporate the RIP information that it receives; when set to <b>None</b> , it will not send any RIP packets and will ignore any RIP packets received.
RIP Version	The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). <b>RIP-1</b> is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both <b>RIP-2B</b> and <b>RIP-2M</b> sends the routing data in RIP-2 format; the difference being that <b>RIP-2B</b> uses subnet broadcasting while <b>RIP-2M</b> uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to <b>Both</b> and the Version set to <b>RIP-1</b> .
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

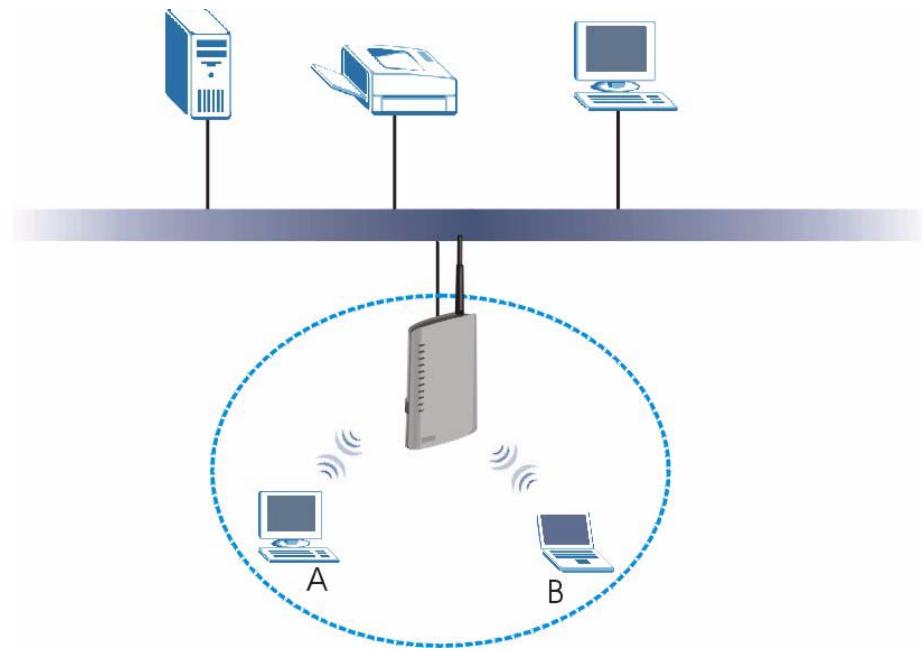
# Wireless LAN

This chapter discusses how to configure the wireless network settings in your ZyXEL Device. See the appendices for more detailed information about wireless networks.

## 9.1 Wireless Network Overview

The following figure provides an example of a wireless network.

**Figure 66** Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your ZyXEL Device is the AP.

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.  
The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use a different channel.

Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.

- Every device in the same wireless network must use security compatible with the AP. Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

## 9.2 Wireless Security Overview

The following sections introduce different types of wireless security you can set up in the wireless network.

### 9.2.1 SSID

Normally, the ZyXEL Device acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the ZyXEL Device does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

### 9.2.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.<sup>2</sup> A MAC address is usually written using twelve hexadecimal characters<sup>3</sup>; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device's User's Guide or other documentation.

You can use the MAC address filter to tell the ZyXEL Device which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized wireless devices to get the MAC address of an authorized device. Then, they can use that MAC address to use the wireless network.

### 9.2.3 User Authentication

Authentication is the process of verifying whether a wireless device is allowed to use the wireless network. You can make every user log in to the wireless network before they can use it. However, every device in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

- 
2. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
  3. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

### 9.2.4 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of authentication. (See [Section 9.2.3 on page 130](#) for information about this.)

**Table 34** Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
<b>Weakest</b> ↑ ↓ <b>Strongest</b>	No Security	WPA
	Static WEP	
	WPA-PSK	
	WPA2-PSK	WPA2

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every device in the wireless network supports. For example, suppose you have a wireless network with the ZyXEL Device and you do not have a RADIUS server. Therefore, there is no authentication. Suppose the wireless network has two devices. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.



It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. The other types of encryption are better than none at all, but it is still possible for unauthorized wireless devices to figure out the original information pretty quickly.

When you select **WPA2** or **WPA2-PSK** in your ZyXEL Device, you can also select an option (**WPA compatible**) to support WPA as well. In this case, if some of the devices support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA compatible** option in the ZyXEL Device.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every device in the wireless network must have the same key.

## 9.2.5 One-Touch Intelligent Security Technology (OTIST)

With ZyXEL's OTIST, you set up the SSID and the encryption (WEP or WPA-PSK) on the ZyXEL Device. Then, the ZyXEL Device transfers them to the devices in the wireless networks. As a result, you do not have to set up the SSID and encryption on every device in the wireless network.

The devices in the wireless network have to support OTIST, and they have to be in range of the ZyXEL Device when you activate it. See [Section 9.6 on page 140](#) for more details.

## 9.3 Wireless Performance Overview

The following sections introduce different ways to improve the performance of the wireless network.

### 9.3.1 Quality of Service (QoS)

You can turn on Wi-Fi MultiMedia (WMM) QoS to improve the performance of voice and video applications in the wireless network. QoS gives high priority to voice and video, which makes them run more smoothly. Similarly, it gives low priority to many large file downloads so that they do not reduce the quality of other applications.

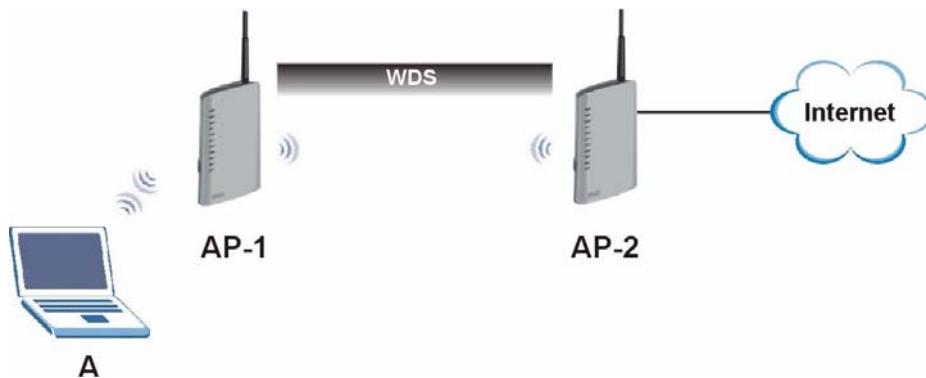
### 9.3.2 Wireless Distribution System (WDS)

The ZyXEL Device can act as a wireless network bridge and establish up to four WDS (Wireless Distribution System) links with other APs. You need to know the MAC addresses of the APs you want to link to. Once the security settings of peer sides match one another, the connection between devices is made.

At the time of writing, WDS security is compatible with other ZyXEL access points only. Refer to your other access point's documentation for details.

The following example illustrates how the WDS link works. Notebook computer **A** is a wireless client connecting to access point **AP-1**. **AP-1** has no wired Internet connection, but can establish a WDS link with access point **AP-2**, which does. When **AP-1** has a WDS link with **AP-2**, the notebook computer can access the Internet through **AP-2**.

**Figure 67** Example of a WDS Link



## 9.4 Additional Wireless Terms

The following table describes wireless network terms and acronyms used in the ZyXEL Device's Web Configurator.

**Table 35** Additional Wireless Terms

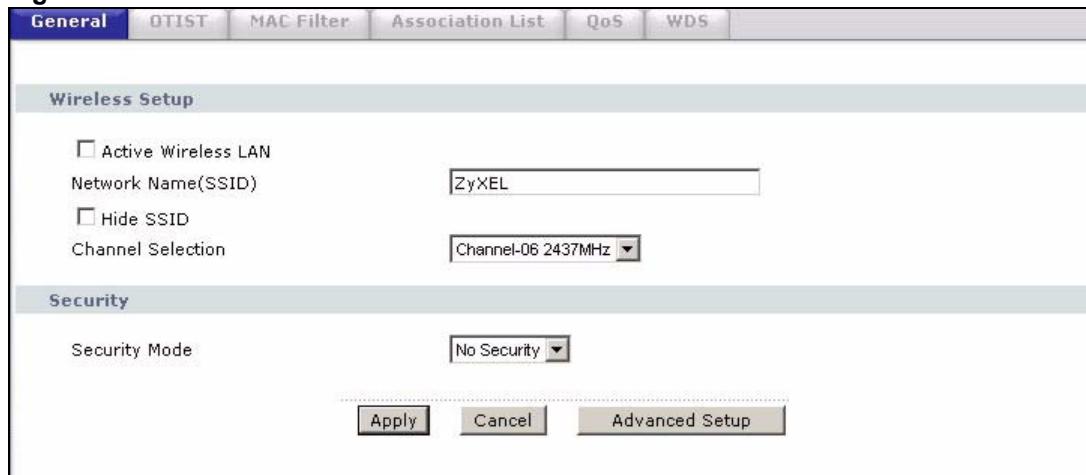
TERM	DESCRIPTION
Intra-BSS Traffic	This describes direct communication (not through the ZyXEL Device) between two wireless devices within a wireless network. You might disable this kind of communication to enhance security within your wireless network.
RTS/CTS Threshold	Use RTS/CTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same AP but out of range of one another. When enabled, a wireless client sends an RTS (Request To Send) and then waits for a CTS (Clear To Send) before it transmits. This stops wireless clients from transmitting packets at the same time (and causing data collisions). A wireless client sends an RTS for all packets larger than the number (of bytes) that you enter here. Set the RTS/CTS equal to or higher than the fragmentation threshold to turn RTS/CTS off.
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the ZyXEL Device does, it cannot communicate with the ZyXEL Device.
Authentication	The process of verifying whether a wireless device is allowed to use the wireless network.
Max. Frame Burst	Enable this to improve the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time that the ZyXEL Device transmits IEEE 802.11g wireless traffic only.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.
Roaming	If you have two or more ZyXEL Devices (or other wireless access points) on your wireless network, you can enable this option so that wireless devices can change locations without having to log in again. This is useful for devices, such as notebooks, that move around a lot.

## 9.5 General WLAN Screen



If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.

Click **Network > Wireless LAN** to open the **Wireless LAN General** screen.

**Figure 68** Wireless LAN: General

The following table describes the labels in this screen.

**Table 36** Wireless LAN: General

LABEL	DESCRIPTION
Active Wireless LAN	Click the check box to activate the wireless LAN.
Network Name (SSID)	(Service Set IDentity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.  Note: If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or WEP settings, you will lose your wireless connection when you press <b>Apply</b> to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Channel Selection	Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box.
Security Mode	See the following sections for more details about this field.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to reload the previous configuration for this screen.
Advanced Setup	Click <b>Advanced Setup</b> to display the <b>Wireless Advanced Setup</b> screen and edit more details of your WLAN setup.

### 9.5.1 No Security

Select **No Security** to allow wireless stations to communicate with the access points without any data encryption.



If you do not enable any wireless security on your ZyXEL Device, your network is accessible to any wireless networking device that is within range.

**Figure 69** Wireless: No Security

The screenshot shows the 'Wireless' configuration interface. At the top, there are tabs: General (selected), OTIST, MAC Filter, Association List, QoS, and WDS. Below the tabs, the 'Wireless Setup' section contains the following fields:

- Active Wireless LAN: Unchecked checkbox.
- Network Name(SSID): Text input field containing "ZyXEL".
- Hide SSID: Unchecked checkbox.
- Channel Selection: A dropdown menu set to "Channel-06 2437MHz".

Below this is the 'Security' section:

- Security Mode: A dropdown menu currently set to "No Security".

At the bottom right are three buttons: "Apply", "Cancel", and "Advanced Setup".

The following table describes the labels in this screen.

**Table 37** Wireless No Security

LABEL	DESCRIPTION
Security Mode	Choose <b>No Security</b> from the drop-down list box.

### 9.5.2 WEP Encryption Screen

Select **Static WEP** from the **Security Mode** list.

**Figure 70** Wireless: Static WEP Encryption

The screenshot shows the 'Wireless' configuration page with the 'General' tab selected. Under 'Wireless Setup', the 'Network Name(SSID)' is set to 'ZyXEL'. Under 'Security', 'Security Mode' is set to 'Static WEP'. There are fields for 'Passphrase' and 'WEP Key'. A note provides instructions for setting the WEP key length (40/64-bit, 128-bit, or 256-bit) and character set (ASCII or hex). At the bottom are 'Apply', 'Cancel', and 'Advanced Setup' buttons.

The following table describes the wireless LAN security labels in this screen.

**Table 38** Wireless: Static WEP Encryption

LABEL	DESCRIPTION
Security Mode	Choose <b>Static WEP</b> from the drop-down list box.
Passphrase	Enter a Passphrase (up to 32 printable characters) and click <b>Generate</b> . The ZyXEL Device automatically generates a WEP key.
WEP Key	The WEP key is used to encrypt data. The ZyXEL Device and all the wireless APs must use the same WEP key for data transmission. If you want to manually set the WEP key, enter any 5, 13 or 29 characters (ASCII string) or 10, 26 or 58 hexadecimal characters ("0-9", "A-F") for a 40/64-bit, 128-bit or 256-bit WEP key respectively.

### 9.5.3 WPA(2)-PSK

In order to configure and enable WPA(2)-PSK authentication; click **Network > Wireless LAN** to display the **General** screen. Select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

**Figure 71** Wireless: WPA(2)-PSK

The screenshot shows the ZyXEL device's Wireless: WPA(2)-PSK configuration screen. The General tab is selected. In the Wireless Setup section, the Network Name (SSID) is set to 'ZyXEL'. Under the Security section, the Security Mode is set to 'WPA2-PSK'. Other security parameters like Pre-Shared Key, ReAuthentication Timer (1800 seconds), Idle Timeout (3600 seconds), and Group Key Update Timer (1800 seconds) are also visible. At the bottom, there are 'Apply', 'Cancel', and 'Advanced Setup' buttons.

The following table describes the wireless LAN security labels in this screen.

**Table 39** Wireless: WPA(2)-PSK

LABEL	DESCRIPTION
Security Mode	Choose <b>WPA-PSK</b> or <b>WPA2-PSK</b> from the drop-down list box.
WPA Compatible	This field is only available for WPA2-PSK. Select this if you want the ZyXEL Device to support WPA-PSK and WPA2-PSK simultaneously.
Pre-Shared Key	The encryption mechanisms used for <b>WPA(2)</b> and <b>WPA(2)-PSK</b> are the same. The only difference between the two is that <b>WPA(2)-PSK</b> uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes).  Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).
Group Key Update Timer	The <b>Group Key Update Timer</b> is the rate at which the AP (if using <b>WPA(2)-PSK</b> key management) or <b>RADIUS</b> server (if using WPA key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the <b>Group Key Update Timer</b> is also supported in <b>WPA-PSK</b> mode. The ZyXEL Device default is <b>1800</b> seconds (30 minutes).

### 9.5.4 WPA(2) Authentication Screen

In order to configure and enable WPA Authentication; click the **Wireless LAN** link under **Network** to display the **Wireless** screen. Select **WPA** or **WPA2** from the **Security Mode** list.

**Figure 72** Wireless: WPA(2)

General		DTIST	MAC Filter	Association List	QoS	WDS	
<b>Wireless Setup</b>							
<input type="checkbox"/> Active Wireless LAN							
Network Name(SSID)	ZyXEL						
<input type="checkbox"/> Hide SSID							
Channel Selection	Channel-06 2437MHz						
<b>Security</b>							
Security Mode	WPA2						
<input type="checkbox"/> WPA Compatible							
ReAuthentication Timer	1800	(In Seconds)					
Idle Timeout	3600	(In Seconds)					
Group Key Update Timer	1800	(In Seconds)					
Authentication Server							
IP Address	0.0.0.0						
Port Number	1812						
Shared Secret							
Accounting Server (optional)							
IP Address	0.0.0.0						
Port Number	1813						
Shared Secret							
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Advanced Setup"/>							

The following table describes the wireless LAN security labels in this screen.

**Table 40** Wireless: WPA(2)

LABEL	DESCRIPTION
Security Mode	Choose <b>WPA</b> or <b>WPA2</b> from the drop-down list box.
WPA Compatible	This field is only available for WPA2. Select this if you want the ZyXEL Device to support WPA and WPA2 simultaneously.
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes).  Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).

**Table 40** Wireless: WPA(2)

LABEL	DESCRIPTION
WPA Group Key Update Timer	The <b>WPA Group Key Update Timer</b> is the rate at which the AP (if using <b>WPA-PSK</b> key management) or <b>RADIUS</b> server (if using WPA key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the <b>WPA Group Key Update Timer</b> is also supported in <b>WPA-PSK</b> mode. The ZyXEL Device default is <b>1800</b> seconds (30 minutes).
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is <b>1812</b> . You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyXEL Device. The key must be the same on the external authentication server and your ZyXEL Device. The key is not sent over the network.
Accounting Server (optional)	
IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	Enter the port number of the external accounting server. The default port number is <b>1813</b> . You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the ZyXEL Device. The key must be the same on the external accounting server and your ZyXEL Device. The key is not sent over the network.

### 9.5.5 Wireless LAN Advanced Setup

To configure advanced wireless settings, click the **Advanced Setup** button in the **General** screen. The screen appears as shown.

**Figure 73** Wireless LAN: Advanced

Wireless Advanced Setup	
RTS/CTS Threshold	2432 (0 ~ 2432, 4096 when G+ Enhanced)
Fragmentation Threshold	2432 (256 ~ 2432, 4096 when G+ Enhanced)
Preamble	Long
802.11 Mode	802.11g Only
<input type="checkbox"/> Enable 802.11g+ mode	
<input type="button" value="Back"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

The following table describes the labels in this screen.

**Table 41** Wireless LAN: Advanced

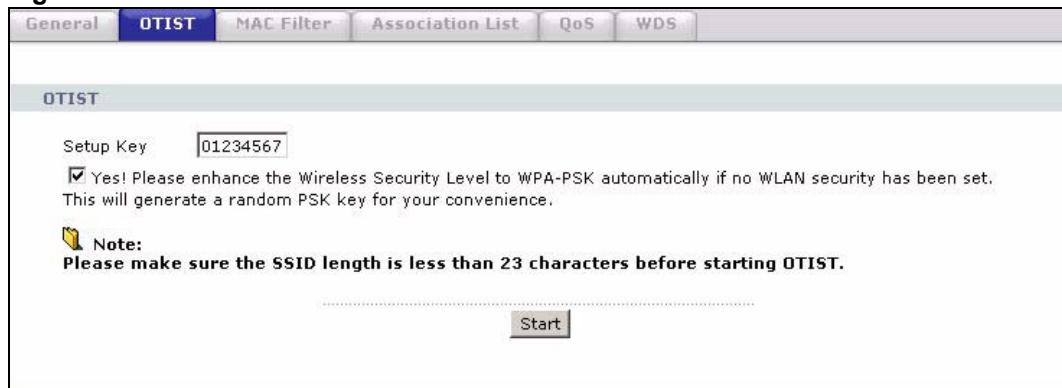
LABEL	DESCRIPTION
Wireless Advanced Setup	
RTS/CTS Threshold	Enter a value between 0 and 2432. If you select the G+ Enhanced checkbox a value of 4096 is displayed.
Fragmentation Threshold	It is the maximum data fragment size that can be sent. Enter a value between 256 and 2432. If you select the G+ Enhanced checkbox a value of 4096 is displayed.
Preamble	Select a preamble type from the drop-down list menu. Choices are <b>Long</b> , <b>Short</b> or <b>Dynamic</b> . The default setting is <b>Long</b> . See the appendix for more information.
802.11 Mode	Select <b>802.11b Only</b> to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyXEL Device. Select <b>802.11g Only</b> to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. Select <b>Mixed</b> to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.
Enable 802.11g+ mode	Select <b>Enable 802.11g+ mode</b> checkbox to allow any ZyXEL WLAN devices that support this feature to associate with the ZyXEL Device at higher transmission speeds. This permits the ZyXEL Device to transmit at a higher speed than the <b>802.11g Only</b> mode.
Back	Click this to return to the previous screen without saving changes.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to reload the previous configuration for this screen.

## 9.6 OTIST Screen

Use this screen to set up and start OTIST on the ZyXEL Device in your wireless network. To open this screen, click **Network > Wireless LAN > OTIST**.



Ensure that your network's SSID is fewer than 23 characters in length before you start OTIST. Click **Wireless LAN > General** to change your network's SSID.

**Figure 74** Network > Wireless LAN > OTIST

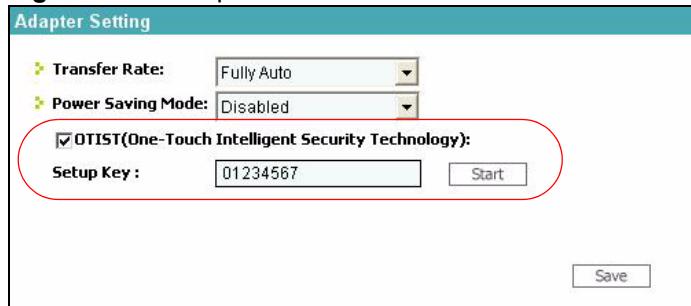
The following table describes the labels in this screen.

**Table 42** Network > Wireless LAN > OTIST

LABEL	DESCRIPTION
Setup Key	Type a key (password) 8 ASCII characters long.  Note: If you change the OTIST setup key in the ZyXEL Device, you must change it on the wireless devices too.
Yes!	Select this if you want the ZyXEL Device to automatically generate a pre-shared key for the wireless network. Before you do this, click <b>Network &gt; Wireless LAN &gt; General</b> and set the <b>Security Mode</b> to <b>No Security</b> . Clear this if you want the ZyXEL Device to use a pre-shared key that you enter. Before you do this, click <b>Network &gt; Wireless LAN &gt; General</b> , set the <b>Security Mode</b> to <b>WPA-PSK</b> , and enter the <b>Pre-Shared Key</b> .
Start	Click <b>Start</b> to activate OTIST and transfer settings. The process takes three minutes to complete.  Note: You must click <b>Start</b> in the ZyXEL Device and in the wireless device(s) within three minutes of each other. You can start OTIST in the wireless devices and the ZyXEL Device in any order.

Before you click **Start**, you should enable OTIST on all the OTIST-enabled devices in the wireless network. For most devices, follow these steps.

- 1 Start the ZyXEL utility
- 2 Click the **Adapter** tab.
- 3 Select the **OTIST** check box, and enter the same **Setup Key** as the ZyXEL Device.
- 4 Click **Save**.

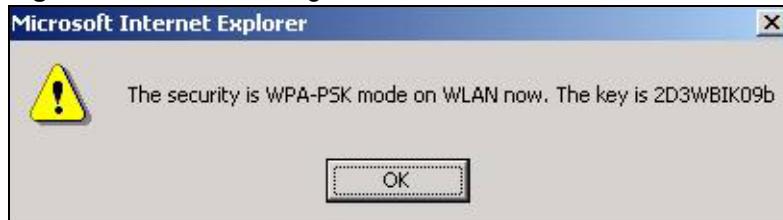
**Figure 75** Example: Wireless Client OTIST Screen

To start OTIST in the device, click **Start** in this screen.



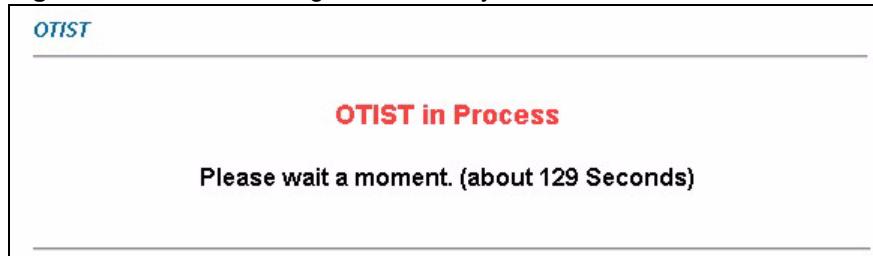
You must click **Start** in the ZyXEL Device and in the wireless device(s) within three minutes of each other. You can start OTIST in the wireless devices and the ZyXEL Device in any order.

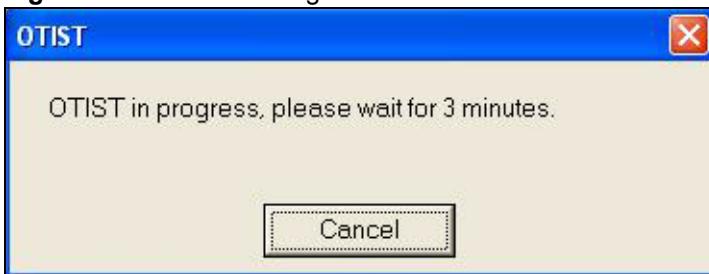
After you click **Start** in the ZyXEL Device, the following screen appears (in the ZyXEL Device).

**Figure 76** OTIST: Settings

You can use the key in this screen to set up WPA-PSK encryption manually for non-OTIST devices in the wireless network.

Review the settings, and click **OK**. The ZyXEL Device begins transferring OTIST settings. The following screens appear in the ZyXEL Device and in the wireless devices.

**Figure 77** OTIST: In Progress on the ZyXEL Device

**Figure 78** OTIST: In Progress on the Wireless Device

These screens close when the transfer is complete.

### 9.6.1 Notes on OTIST

- 1 If you enable OTIST in a wireless device, you see this screen each time you start the utility. Click **Yes** to search for an OTIST-enabled AP (in other words, the ZyXEL Device).

**Figure 79** Start OTIST?

- 2 If an OTIST-enabled wireless device loses its wireless connection for more than ten seconds, it will search for an OTIST-enabled AP for up to one minute. (If you manually have the wireless device search for an OTIST-enabled AP, there is no timeout; click **Cancel** in the OTIST progress screen to stop the search.)
- 3 After the wireless device finds an OTIST-enabled AP, you must click **Start** in the ZyXEL Device's **Network > Wireless LAN > OTIST** screen or hold in the **Reset** button on the ZyXEL Device for one or two seconds to transfer the settings again.
- 4 If you change the SSID or the keys on the ZyXEL Devices after using OTIST, you need to run OTIST again or enter them manually in the wireless device(s).
- 5 If you configure OTIST to generate a WPA-PSK key, this key changes each time you run OTIST. Therefore, if a new wireless device joins your wireless network, you need to run OTIST on the AP and ALL wireless devices again.

## 9.7 MAC Filter

Use this screen to change your ZyXEL Device's MAC filter settings. MAC filtering lets you control which devices can access the ZyXEL Device and the network. You can allow or prohibit specific devices based on their MAC addresses. Click **Network > Wireless LAN > MAC Filter**. The screen appears as shown.

**Figure 80** MAC Address Filter

Set	MAC Address	Set	MAC Address
1	00:12:f0:e8:dc:b3	2	00:00:00:00:00:00
3	00:00:00:00:00:00	4	00:00:00:00:00:00
5	00:00:00:00:00:00	6	00:00:00:00:00:00
7	00:00:00:00:00:00	8	00:00:00:00:00:00
9	00:00:00:00:00:00	10	00:00:00:00:00:00
11	00:00:00:00:00:00	12	00:00:00:00:00:00
13	00:00:00:00:00:00	14	00:00:00:00:00:00
15	00:00:00:00:00:00	16	00:00:00:00:00:00
17	00:00:00:00:00:00	18	00:00:00:00:00:00
19	00:00:00:00:00:00	20	00:00:00:00:00:00
21	00:00:00:00:00:00	22	00:00:00:00:00:00
23	00:00:00:00:00:00	24	00:00:00:00:00:00
25	00:00:00:00:00:00	26	00:00:00:00:00:00
27	00:00:00:00:00:00	28	00:00:00:00:00:00
29	00:00:00:00:00:00	30	00:00:00:00:00:00
31	00:00:00:00:00:00	32	00:00:00:00:00:00

**Apply**    **Cancel**

The following table describes the labels in this screen.

**Table 43** MAC Address Filter

LABEL	DESCRIPTION
Active MAC Filter	Select the check box to enable MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the <b>MAC Address</b> table. Select <b>Deny</b> to block access to the ZyXEL Device, MAC addresses not listed will be allowed to access the ZyXEL Device. Select <b>Allow</b> to permit access to the ZyXEL Device, MAC addresses not listed will be denied access to the ZyXEL Device.
Set	This is the index number of the MAC address.
MAC Address	Enter the MAC addresses of the wireless station that are allowed or denied access to the ZyXEL Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to reload the previous configuration for this screen.

## 9.8 Association List

Use this screen to view details of the wireless stations that are currently associated with the ZyXEL Device. You can also block individual wireless stations from accessing the network through the ZyXEL Device.

Click **Network > Wireless LAN > Association List** to display the screen as shown next.

**Figure 81** Wireless LAN: Association List

General	DTIST	MAC Filter	Association List	QoS	WDS
<b>Association List - MAC Filter</b>					
#	MAC Address	Association Time	Deny		
001	00:12:f0:e8:dc:b3	01:44:20 2000/01/01	<input type="checkbox"/>		
<b>Apply</b>					<b>Cancel</b>

The following table describes the labels in this screen.

**Table 44** Wireless LAN: Association List

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of a wireless station that is currently associated with the ZyXEL Device.
Association Time	When a wireless station is accessing the ZyXEL Device, this field displays the time (hh:mm:ss) (yyyy/mm/dd) of when the association starts. The time synchronizes with the time server.
Deny	Select this to add this MAC address to the <b>MAC Filter</b> blocking list. The device with this MAC address can no longer associate with the ZyXEL Device.  If the MAC filter is not activated, this action enables the MAC filter with the filter action set to <b>Deny</b> .  <b>Note:</b> If a MAC address is on the <b>MAC Filter</b> non-blocking list (when MAC filter is activated and the filter action is set to <b>Allow</b> ), you cannot deny it in the <b>Association List</b> screen.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to reload the previous configuration for this screen.

## 9.9 QoS Screen

The QoS screen allows you to automatically give a service (such as e-mail, VoIP or FTP) a priority level.

Click **Network > Wireless LAN > QoS**. The following screen displays.

**Figure 82** Wireless LAN: QoS

#	Name	Service	Dest Port	Priority	Modify
1	-	-	0	-	
2	-	-	0	-	
3	-	-	0	-	
4	-	-	0	-	
5	-	-	0	-	
6	-	-	0	-	
7	-	-	0	-	
8	-	-	0	-	
9	-	-	0	-	
10	-	-	0	-	

**QoS**

Enable WMM QoS

WMM QoS Policy: Application Priority

Buttons: Apply, Cancel

The following table describes the fields in this screen.

**Table 45** Wireless LAN: QoS

LABEL	DESCRIPTION
QoS Setup	
Enable WMM QoS	Select the check box to enable WMM QoS on the ZyXEL Device.
WMM QoS Policy	Select <b>Default</b> to have the ZyXEL Device automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly. Select <b>Application Priority</b> from the drop-down list box to display a table of application names, services, ports and priorities to which you want to apply WMM QoS.
	The table appears only if you select <b>Application Priority</b> in <b>WMM QoS Policy</b> .
#	This is the number of an individual application entry.
Name	This field displays a description given to an application entry.
Service	This field displays either <b>FTP</b> , <b>WWW</b> , <b>E-mail</b> or a <b>User Defined</b> service to which you want to apply WMM QoS.
Dest Port	This field displays the destination port number to which the application sends traffic.
Priority	This field displays the priority of the application. <b>Highest</b> - Typically used for voice or video that should be high-quality. <b>High</b> - Typically used for voice or video that can be medium-quality. <b>Mid</b> - Typically used for applications that do not fit into another priority. For example, Internet surfing. <b>Low</b> - Typically used for non-critical "background" applications, such as large file transfers and print jobs that should not affect other applications.

**Table 45** Wireless LAN: QoS

LABEL	DESCRIPTION
Modify	Click the <b>Edit</b> icon to open the <b>Application Priority Configuration</b> screen. Modify an existing application entry or create a application entry in the <b>Application Priority Configuration</b> screen. Click the <b>Remove</b> icon to delete an application entry.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.

### 9.9.1 Application Priority Configuration

Use this screen to edit a WMM QoS application entry. Click the edit icon under **Modify**. The following screen displays.

**Figure 83** Application Priority Configuration

The screenshot shows a configuration dialog titled "Application Priority Configuration". It contains the following fields:

- Name: (empty input field)
- Service: (dropdown menu showing "E-Mail")
- Dest Port: (input field showing "25")
- Priority: (dropdown menu showing "Highest")

At the bottom are two buttons: "Apply" and "Cancel".

See [Appendix E on page 475](#) for a list of commonly-used services and destination ports. The following table describes the fields in this screen.

**Table 46** Application Priority Configuration

LABEL	DESCRIPTION
Application Priority Configuration	
Name	Type a description of the application priority.

**Table 46** Application Priority Configuration

LABEL	DESCRIPTION
Service	The following is a description of the applications you can prioritize with WMM QoS. Select a service from the drop-down list box. <ul style="list-style-type: none"> <li>• <b>E-Mail</b> Electronic mail consists of messages sent through a computer network to specific groups or individuals. Here are some default ports for e-mail: POP3 - port 110 IMAP - port 143 SMTP - port 25 HTTP - port 80</li> <li>• <b>FTP</b> File Transfer Protocol enables fast transfer of files, including large files that it may not be possible to send via e-mail. FTP uses port number 21.</li> <li>• <b>WWW</b> The World Wide Web is an Internet system to distribute graphical, hyper-linked information, based on Hyper Text Transfer Protocol (HTTP) - a client/server protocol for the World Wide Web. The Web is not synonymous with the Internet; rather, it is just one service on the Internet. Other services on the Internet include Internet Relay Chat and Newsgroups. The Web is accessed through use of a browser.</li> <li>• <b>User-Defined</b> User-defined services are user specific services configured using known ports and applications.</li> </ul>
Dest Port	This displays the port the selected service uses. Type a port number in the field provided if you want to use a different port to the default port.
Priority	Select a priority from the drop-down list box.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to return to the previous screen.

## 9.10 WDS Screen

Use this screen to set up your WDS (Wireless Distribution System) links between the ZyXEL Device and other wireless APs. You need to know the MAC address of the peer device. Once the security settings of peer sides match one another, the connection between devices is made. At the time of writing, the ZyXEL Device can support up to four WDS links at the same time.



WDS security is independent of the security settings between the ZyXEL Device and any wireless clients. Check your other AP's documentation to make sure it supports WDS security.

Click **Network > Wireless LAN > WDS**. The following screen displays.

**Figure 84** Wireless LAN > WDS

#	Active	MAC Address
1	<input type="checkbox"/>	00:00:00:00:00:00
2	<input type="checkbox"/>	00:00:00:00:00:00
3	<input type="checkbox"/>	00:00:00:00:00:00
4	<input type="checkbox"/>	00:00:00:00:00:00

**Security**

Security Mode: No Security

Buttons: Apply, Cancel

The following table describes the fields in this screen.

**Table 47** Wireless LAN > WDS

LABEL	DESCRIPTION
Remote Bridge MAC Address	
#	This is the index number of the individual WDS link.
Active	Select this to activate the link between the ZyXEL Device and the peer device to which this entry refers. When you do not select the check box this link is down.
MAC Address	Type the MAC address of the peer device in a valid MAC address format, six hexadecimal character pairs, 12:34:56:78:9a:bc, for example.
Security	
Security Mode	<p>Select one of the security settings.</p> <ul style="list-style-type: none"> <li>• <b>No Security</b></li> <li>• <b>Static WEP</b></li> <li>• <b>WPA-PSK</b></li> <li>• <b>WPA2-PSK</b></li> </ul> <p>If you select <b>No Security</b>, the data sent between APs is not encrypted. Anyone can read it. See the following sections for more information.</p> <p><b>Note: Other APs must use the same encryption method on security settings to enable WDS security.</b></p>
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to return to the previous screen.

### 9.10.1 Static WEP

Choose **Static WEP** from the **Security Mode** list.

**Figure 85** Wireless LAN > WDS > Static WEP

#	Active	MAC Address
1	<input type="checkbox"/>	00:00:00:00:00:00
2	<input type="checkbox"/>	00:00:00:00:00:00
3	<input type="checkbox"/>	00:00:00:00:00:00
4	<input type="checkbox"/>	00:00:00:00:00:00

**Security**

Security Mode: Static WEP

WEP Key:

**Note:**  
The different WEP key lengths configure different strength security, 40/64-bit, 128-bit, or 256-bit respectively. Your wireless client must match the security strength set on the router.  
-Please type exactly 5, 13, or 29 characters.  
or  
-Please type exactly 10, 26, or 58 characters using only the numbers 0-9 and the letters 'a-f' or 'A-F'.

.....

**Apply**    **Cancel**

The following table describes the labels in this screen.

**Table 48** Wireless LAN > WDS > Static WEP

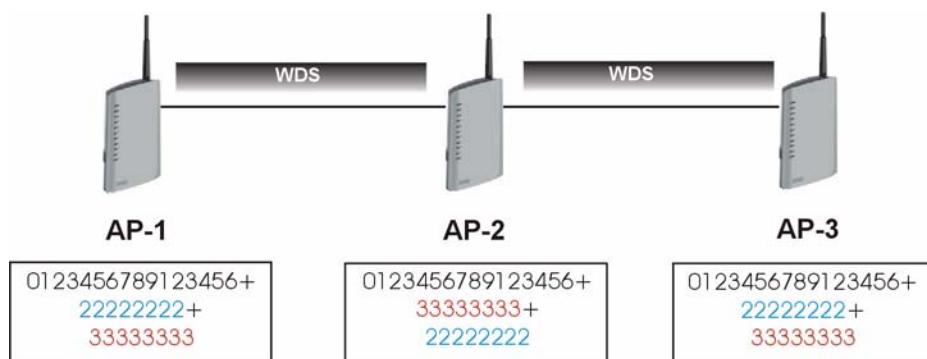
LABEL	DESCRIPTION
Security Mode	Choose <b>Static WEP</b> from the drop-down list box.
WEP Key	The WEP key is used to encrypt data. All of the wireless APs (including the ZyXEL Device) must use the same WEP key for data transmission. Enter any 5, 13 or 29 characters (ASCII string) or 10, 26 or 58 hexadecimal characters ("0-9", "A-F") for a 40/64-bit, 128-bit or 256-bit WEP key respectively.

## 9.10.2 WPA-PSK

The WPA-PSK Pre-Shared Key standard uses TKIP (Temporal Key Integrity Protocol) encryption. When you choose this, the Pre-Shared Key you enter must have the following format:

- Sixteen-character common key (**common**): all APs in the WDS share the same common key. All ASCII characters (including spaces and symbols) are allowed.
- Eight-character transmission key (**tx**): this must be the same as the next AP's reception key. All ASCII characters (including spaces and symbols) are allowed.
- Eight-character reception key (**rx**): this must be the same as the next AP's transmission key. All ASCII characters (including spaces and symbols) are allowed.
- The common, transmission key and reception key are connected by '+' the plus sign.

The following example shows how to set up a WDS link between wireless APs using WPA-PSK with TKIP.

**Figure 86** Example: WDS Link using WPA-PSK with TKIP

- **AP-1, AP-2 and AP-3** share the same common key “0123456789123456”.
- The transmission key “22222222” of **AP-1** is exactly the same as the reception key “22222222” of **AP-2**.
- The transmission key “33333333” of **AP-2** is exactly the same as the reception key “33333333” of **AP-3**.

To access this screen, choose **WPA-PSK** from the **Security Mode** list.

**Figure 87** Wireless LAN > WDS > WPA-PSK

General	OTIST	MAC Filter	Association List	QoS	<b>WDS</b>															
<p><b>Remote Bridge MAC Address</b></p> <table border="1"> <thead> <tr> <th>#</th> <th>Active</th> <th>MAC Address</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input type="checkbox"/></td> <td>00:00:00:00:00:00</td> </tr> <tr> <td>2</td> <td><input type="checkbox"/></td> <td>00:00:00:00:00:00</td> </tr> <tr> <td>3</td> <td><input type="checkbox"/></td> <td>00:00:00:00:00:00</td> </tr> <tr> <td>4</td> <td><input type="checkbox"/></td> <td>00:00:00:00:00:00</td> </tr> </tbody> </table> <p><b>Security</b></p> <p>Security Mode: <b>WPA-PSK</b> <input type="button" value="▼"/></p> <p>Pre-Shared Key: <input type="text"/></p> <p><b>Note:</b> TKIP:16 characters (common)+8 characters(tx)+8 characters(rx).</p> <p style="text-align: right;"><b>Apply</b> <b>Cancel</b></p>						#	Active	MAC Address	1	<input type="checkbox"/>	00:00:00:00:00:00	2	<input type="checkbox"/>	00:00:00:00:00:00	3	<input type="checkbox"/>	00:00:00:00:00:00	4	<input type="checkbox"/>	00:00:00:00:00:00
#	Active	MAC Address																		
1	<input type="checkbox"/>	00:00:00:00:00:00																		
2	<input type="checkbox"/>	00:00:00:00:00:00																		
3	<input type="checkbox"/>	00:00:00:00:00:00																		
4	<input type="checkbox"/>	00:00:00:00:00:00																		

The following table describes the labels in this screen.

**Table 49** Wireless LAN > WDS > WPA-PSK

LABEL	DESCRIPTION
Security Mode	Choose <b>WPA-PSK</b> from the drop-down list box.
Pre-Shared Key	<p>The Pre-Shared key (PSK) is used to encrypt data. All the wireless APs (including the ZyXEL Device) must use the same WPA Pre-Shared Key for data transmission.</p> <p>When you choose this, the Pre-Share Key you enter must have the following format:</p> <ul style="list-style-type: none"> <li>• Sixteen-character common key (<b>common</b>): all APs in the WDS share the same common key. All ASCII characters (including spaces and symbols) are allowed.</li> <li>• Eight-character transmission key (<b>tx</b>): this must be the same as the next AP's reception key. All ASCII characters (including spaces and symbols) are allowed.</li> <li>• Eight-character reception key (<b>rx</b>): this must be the same as the next AP's transmission key. All ASCII characters (including spaces and symbols) are allowed.</li> <li>• The common, transmission key and reception key are connected by '+' the plus sign.</li> </ul>

### 9.10.3 WPA2-PSK

Choose **WPA2-PSK** from the **Security Mode** list.

**Figure 88** Wireless LAN > WDS > WPA2-PSK

#	Active	MAC Address
1	<input type="checkbox"/>	00:00:00:00:00:00
2	<input type="checkbox"/>	00:00:00:00:00:00
3	<input type="checkbox"/>	00:00:00:00:00:00
4	<input type="checkbox"/>	00:00:00:00:00:00

**Security**

Security Mode: WPA2-PSK

Pre-Shared Key:

**Note:**  
AES:16 characters.

Buttons: Apply, Cancel

The following table describes the labels in this screen.

**Table 50** Wireless LAN > WDS > WPA2-PSK

LABEL	DESCRIPTION
Security Mode	Choose <b>WPA-PSK</b> from the drop-down list box.
Pre-Shared Key	The Pre-Shared key (PSK) is used to encrypt data. All the wireless APs (including the ZyXEL Device) must use the same Pre-Shared key for data transmission. Enter a Pre-Shared key that consists of 16 ASCII characters (including spaces and symbols).



# Network Address Translation (NAT) Screens

This chapter discusses how to configure NAT on the ZyXEL Device.

## 10.1 NAT General Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

### 10.1.1 NAT Definitions

Inside/outside denotes where a host is located relative to the ZyXEL Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

**Table 51** NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside host.

### 10.1.2 What NAT Does

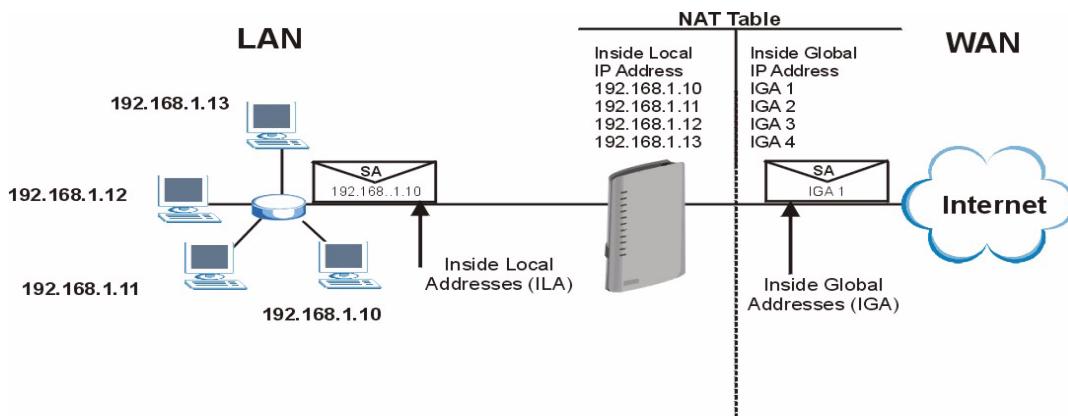
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see [Table 52 on page 158](#)), NAT offers the additional benefit of firewall protection. With no servers defined, your ZyXEL Device filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

### 10.1.3 How NAT Works

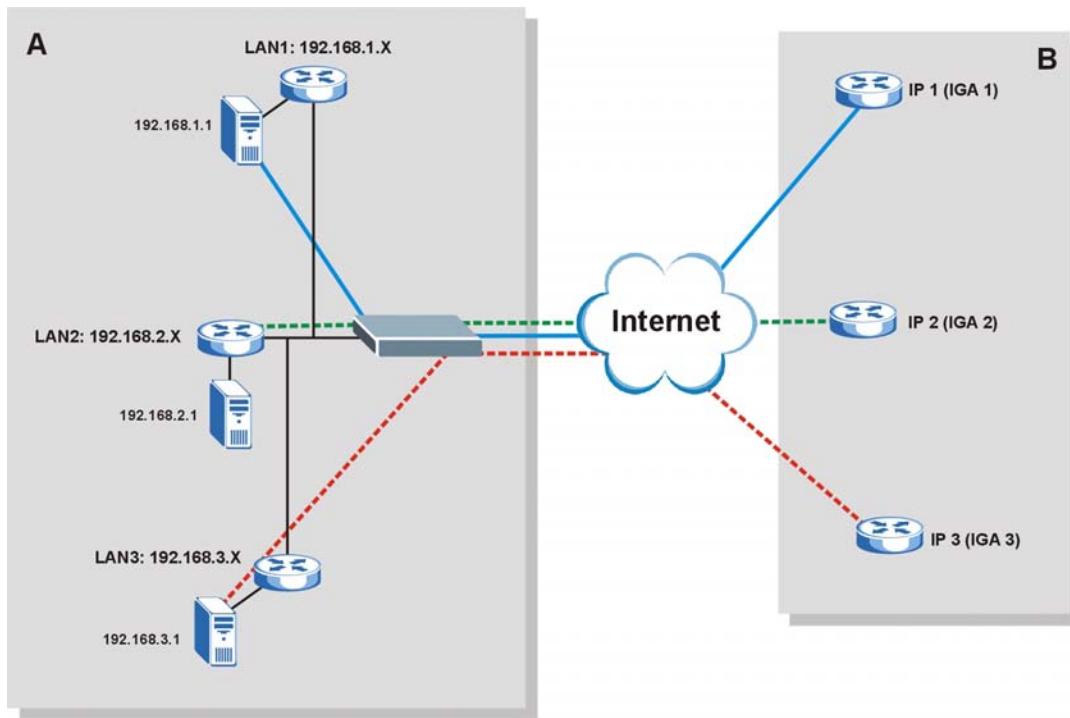
Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The ZyXEL Device keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

**Figure 89** How NAT Works



### 10.1.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the ZyXEL Device can communicate with three distinct WAN networks.

**Figure 90** NAT Application With IP Alias

### 10.1.5 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

- **One to One:** In One-to-One mode, the ZyXEL Device maps one local IP address to one global IP address.
- **Many to One:** In Many-to-One mode, the ZyXEL Device maps multiple local IP addresses to one global IP address. This is equivalent to SUA (for instance, PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported (the **SUA Only** option in today's routers).
- **Many to Many Overload:** In Many-to-Many Overload mode, the ZyXEL Device maps the multiple local IP addresses to shared global IP addresses.
- **Many-to-Many No Overload:** In Many-to-Many No Overload mode, the ZyXEL Device maps each local IP address to a unique global IP address.
- **Server:** This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

Port numbers do NOT change for **One-to-One** and **Many-to-Many No Overload** NAT mapping types.

The following table summarizes these types.

**Table 52** NAT Mapping Types

TYPE	IP MAPPING
One-to-One	ILA1 ↔ IGA1
Many-to-One (SUA/PAT)	ILA1 ↔ IGA1 ILA2 ↔ IGA1 ...
Many-to-Many Overload	ILA1 ↔ IGA1 ILA2 ↔ IGA2 ILA3 ↔ IGA1 ILA4 ↔ IGA2 ...
Many-to-Many No Overload	ILA1 ↔ IGA1 ILA2 ↔ IGA2 ILA3 ↔ IGA3 ...
Server	Server 1 IP ↔ IGA1 Server 2 IP ↔ IGA1 Server 3 IP ↔ IGA1

## 10.2 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The ZyXEL Device also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in [Table 52 on page 158](#).

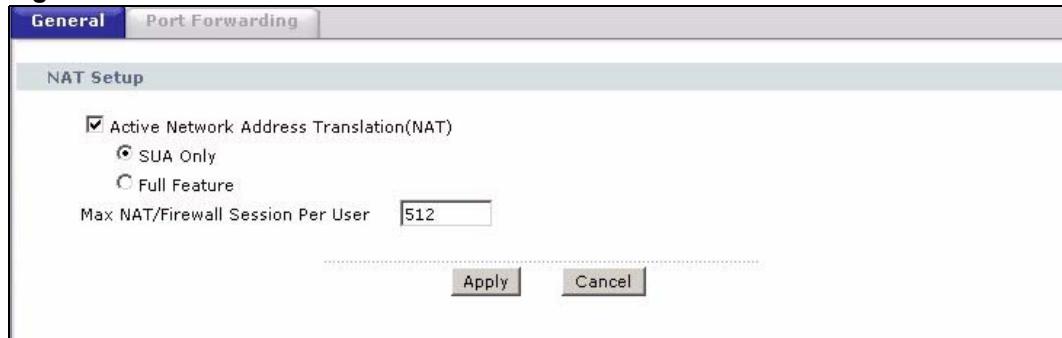
- Choose **SUA Only** if you have just one public WAN IP address for your ZyXEL Device.
  - Choose **Full Feature** if you have multiple public WAN IP addresses for your ZyXEL Device.

## 10.3 NAT General Setup



You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the ZyXEL Device.

Click **Network > NAT** to open the following screen.

**Figure 91** NAT General

The following table describes the labels in this screen.

**Table 53** NAT General

LABEL	DESCRIPTION
Active Network Address Translation (NAT)	Select this check box to enable NAT.
SUA Only	Select this radio button if you have just one public WAN IP address for your ZyXEL Device.
Full Feature	Select this radio button if you have multiple public WAN IP addresses for your ZyXEL Device.
Max NAT/ Firewall Session Per User	When computers use peer to peer applications, such as file sharing applications, they need to establish NAT sessions. If you do not limit the number of NAT sessions a single client can establish, this can result in all of the available NAT sessions being used. In this case, no additional NAT sessions can be established, and users may not be able to access the Internet. Each NAT session establishes a corresponding firewall session. Use this field to limit the number of NAT/Firewall sessions client computers can establish through the ZyXEL Device. If your network has a small number of clients using peer to peer applications, you can raise this number to ensure that their performance is not degraded by the number of NAT sessions they can establish. If your network has a large number of users using peer to peer applications, you can lower this number to ensure no single client is exhausting all of the available NAT sessions.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to reload the previous configuration for this screen.

## 10.4 Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

### 10.4.1 Default Server IP Address

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.



If you do not assign a **Default Server** IP address, the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.

### 10.4.2 Port Forwarding: Services and Port Numbers

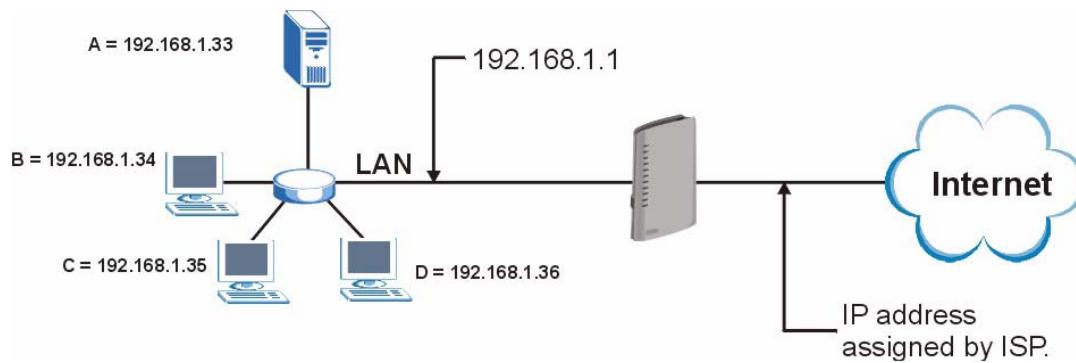
Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network.

The most often used port numbers and services are shown in [Appendix E on page 475](#). Please refer to RFC 1700 for further information about port numbers.

### 10.4.3 Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

**Figure 92** Multiple Servers Behind NAT Example



## 10.5 Configuring Port Forwarding



If you do not assign a **Default Server** IP address, the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.

Click **Network > NAT > Port Forwarding** to open the following screen. This screen is available only when you select **SUA only** in the **NAT > General** screen.

See [Appendix E](#) on page 475 for port numbers commonly used for particular services.

**Figure 93** Port Forwarding

#	Active	Service Name	Start Port	End Port	Server IP Address	Modify
		WWW	80	80		

The following table describes the fields in this screen.

**Table 54** Port Forwarding

LABEL	DESCRIPTION
Default Server Setup	
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a <b>Default Server</b> IP address, the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.
Port Forwarding	
Service Name	Select a service from the drop-down list box.
Server IP Address	Enter the IP address of the server for the specified service.
Add	Click this button to add a rule to the table below.
#	This is the rule index number (read-only).
Active	Click this check box to enable the rule.
Service Name	This is a service's name.
Start Port	This is the first port number that identifies a service.
End Port	This is the last port number that identifies a service.

**Table 54** Port Forwarding

LABEL	DESCRIPTION
Server IP Address	This is the server's IP address.
Modify	Click the edit icon to go to the screen where you can edit the port forwarding rule. Click the delete icon to delete an existing port forwarding rule. Note that subsequent address mapping rules move up by one when you take this action.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to return to the previous configuration.

### 10.5.1 Port Forwarding Rule Edit

Use this screen to edit a port forwarding rule. Click the rule's edit icon in the **Port Forwarding** screen to display the screen shown next.

**Figure 94** Port Forwarding Rule Setup

The screenshot shows a 'Rule Setup' window with the following configuration:

- Active:** Checked checkbox.
- Service Name:** Text input field containing "WWW".
- Start Port:** Text input field containing "80".
- End Port:** Text input field containing "80".
- Server IP Address:** Text input field containing "10.10.1.2".

At the bottom of the window are three buttons: **Back**, **Apply**, and **Cancel**.

The following table describes the fields in this screen.

**Table 55** Port Forwarding Rule Setup

LABEL	DESCRIPTION
Active	Click this check box to enable the rule.
Service Name	Enter a name to identify this port-forwarding rule.
Start Port	Enter a port number in this field. To forward only one port, enter the port number again in the <b>End Port</b> field. To forward a series of ports, enter the start port number here and the end port number in the <b>End Port</b> field.
End Port	Enter a port number in this field. To forward only one port, enter the port number again in the <b>Start Port</b> field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the <b>Start Port</b> field above.
Server IP Address	Enter the inside IP address of the server here.
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 10.6 Address Mapping



The **Address Mapping** screen is available only when you select **Full Feature** in the **NAT > General** screen.

Ordering your rules is important because the ZyXEL Device applies the rules in the order that you specify. When a rule matches the current packet, the ZyXEL Device takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9. Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so old rules 5, 6 and 7 become new rules 4, 5 and 6.

To change your ZyXEL Device's address mapping settings, click **Network > NAT > Address Mapping** to open the following screen.

**Figure 95** Address Mapping Rules

Address Mapping Rules						
#	Local Start IP	Local End IP	Global Start IP	Global End IP	Type	Modify
1	-	-	-	-	-	
2	-	-	-	-	-	
3	-	-	-	-	-	
4	-	-	-	-	-	
5	-	-	-	-	-	
6	-	-	-	-	-	
7	-	-	-	-	-	
8	-	-	-	-	-	
9	-	-	-	-	-	
10	-	-	-	-	-	

The following table describes the fields in this screen.

**Table 56** Address Mapping Rules

LABEL	DESCRIPTION
#	This is the rule index number.
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are <b>N/A</b> for <b>Server</b> port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the <b>Local Start IP</b> address and 255.255.255.255 as the <b>Local End IP</b> address. This field is <b>N/A</b> for <b>One-to-one</b> and <b>Server</b> mapping types.

**Table 56** Address Mapping Rules (continued)

LABEL	DESCRIPTION
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for <b>Many-to-One</b> and <b>Server</b> mapping types.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is <b>N/A</b> for <b>One-to-one</b> , <b>Many-to-One</b> and <b>Server</b> mapping types.
Type	<b>1-1:</b> One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. <b>M-1:</b> Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. <b>M-M Ov</b> (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. <b>MM No</b> (No Overload): Many-to-Many No Overload mode maps each local IP address to unique global IP addresses. <b>Server:</b> This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Modify	Click the edit icon to go to the screen where you can edit the address mapping rule. Click the delete icon to delete an existing address mapping rule. Note that subsequent address mapping rules move up by one when you take this action.

### 10.6.1 Address Mapping Rule Edit

To edit an address mapping rule, click the rule's edit icon in the **Address Mapping** screen to display the screen shown next.

**Figure 96** Edit Address Mapping Rule

The screenshot shows the 'Edit Address Mapping Rule' interface. At the top is a title bar labeled 'Edit Address Mapping Rule1'. Below it are several input fields and dropdown menus:

- Type: A dropdown menu set to 'One-to-One'.
- Local Start IP: An input field containing '0.0.0.0'.
- Local End IP: An input field containing 'N/A'.
- Global Start IP: An input field containing '0.0.0.0'.
- Global End IP: An input field containing 'N/A'.
- Server Mapping Set: A dropdown menu showing '2' with a link 'Edit Details' next to it.

At the bottom of the screen are three buttons: 'Back', 'Apply', and 'Cancel'.

The following table describes the fields in this screen.

**Table 57** Edit Address Mapping Rule

LABEL	DESCRIPTION
Type	Choose the port mapping type from one of the following. <b>One-to-One</b> : One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type. <b>Many-to-One</b> : Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. <b>Many-to-Many Overload</b> : Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. <b>Many-to-Many No Overload</b> : Many-to-Many No Overload mode maps each local IP address to unique global IP addresses. <b>Server</b> : This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting local IP address (ILA). Local IP addresses are <b>N/A</b> for <b>Server</b> port mapping.
Local End IP	This is the end local IP address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the <b>Local Start IP</b> address and 255.255.255.255 as the <b>Local End IP</b> address. This field is <b>N/A</b> for <b>One-to-One</b> and <b>Server</b> mapping types.
Global Start IP	This is the starting global IP address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending global IP address (IGA). This field is <b>N/A</b> for <b>One-to-One</b> , <b>Many-to-One</b> and <b>Server</b> mapping types.
Server Mapping Set	Only available when <b>Type</b> is set to <b>Server</b> . Select a number from the drop-down menu to choose a port forwarding set.
Edit Details	Click this link to go to the <b>Port Forwarding</b> screen to edit a port forwarding set that you have selected in the <b>Server Mapping Set</b> field.
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save your changes to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.



---

# PART IV

# VoIP

---

Voice (169)  
VoIP Trunking (211)  
Phone Usage (227)



# Voice

This chapter provides background information on VoIP and SIP and explains how to configure your device's voice settings.

## 11.1 Introduction to VoIP

VoIP is the sending of voice signals over Internet Protocol. This allows you to make phone calls and send faxes over the Internet at a fraction of the cost of using the traditional circuit-switched telephone network. You can also use servers to run telephone service applications like PBX services and voice mail. Internet Telephony Service Provider (ITSP) companies provide VoIP service.

Circuit-switched telephone networks require 64 kilobits per second (Kbps) in each direction to handle a telephone call. VoIP can use advanced voice coding techniques with compression to reduce the required bandwidth.

## 11.2 SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

### 11.2.1 SIP Identities

A SIP account uses an identity (sometimes referred to as a SIP address). A complete SIP identity is called a SIP URI (Uniform Resource Identifier). A SIP account's URI identifies the SIP account in a way similar to the way an e-mail address identifies an e-mail account. The format of a SIP identity is SIP-Number@SIP-Service-Domain.

#### 11.2.1.1 SIP Number

The SIP number is the part of the SIP URI that comes before the “@” symbol. A SIP number can use letters like in an e-mail address (johndoe@your-ITSP.com for example) or numbers like a telephone number (1122334455@VoIP-provider.com for example).

### 11.2.1.2 SIP Service Domain

The SIP service domain of the VoIP service provider is the domain name in a SIP URI. For example, if the SIP address is [1122334455@VoIP-provider.com](mailto:1122334455@VoIP-provider.com), then “VoIP-provider.com” is the SIP service domain.

### 11.2.2 SIP Servers

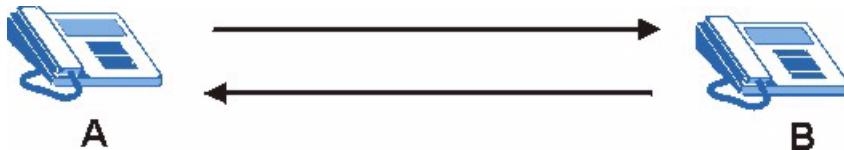
SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

When you use SIP to make a VoIP call, it originates at a client and terminates at a server. A SIP client could be a computer or a SIP phone. One device can act as both a SIP client and a SIP server.

#### 11.2.2.1 SIP User Agent

A SIP user agent can make and receive VoIP telephone calls. This means that SIP can be used for peer-to-peer communications even though it is a client-server protocol. In the following figure, either A or B can act as a SIP user agent client to initiate a call. A and B can also both act as a SIP user agent to receive the call.

**Figure 97** SIP User Agent

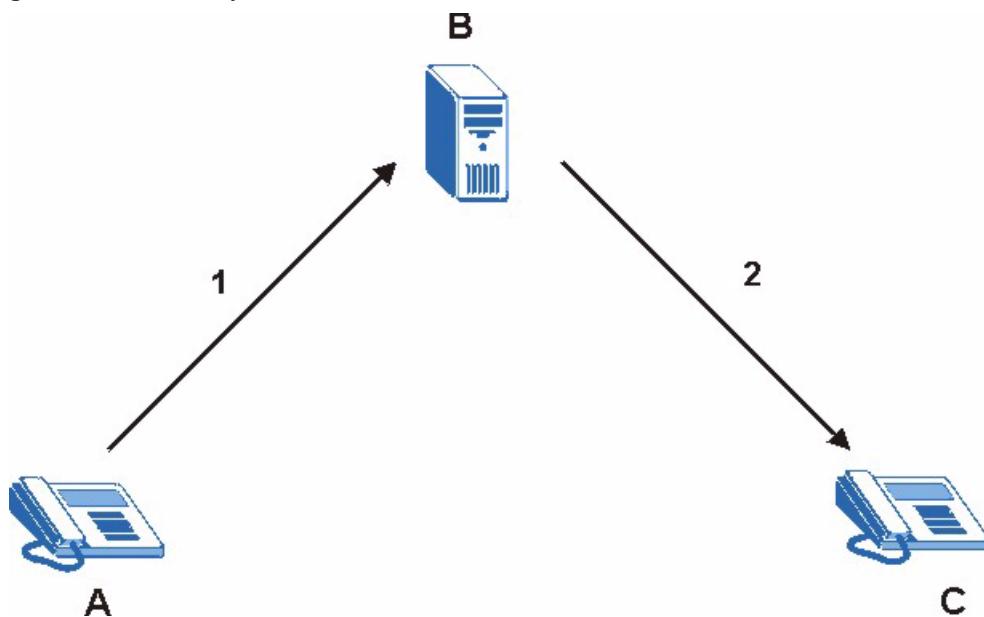


#### 11.2.2.2 SIP Proxy Server

A SIP proxy server receives requests from clients and forwards them to another server.

In the following example, you want to use client device A to call someone who is using client device C.

- 1 The client device (A in the figure) sends a call invitation to the SIP proxy server (B).
- 2 The SIP proxy server forwards the call invitation to C.

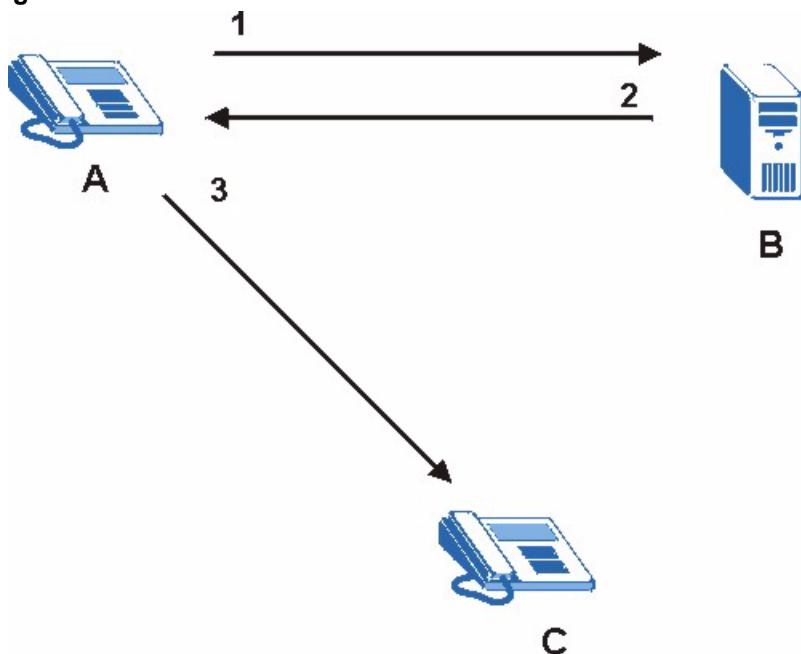
**Figure 98** SIP Proxy Server

#### 11.2.2.3 SIP Redirect Server

A SIP redirect server accepts SIP requests, translates the destination address to an IP address and sends the translated IP address back to the device that sent the request. Then the client device that originally sent the request can send requests to the IP address that it received back from the redirect server. Redirect servers do not initiate SIP requests.

In the following example, you want to use client device A to call someone who is using client device C.

- 1 Client device A sends a call invitation for C to the SIP redirect server (B).
- 2 The SIP redirect server sends the invitation back to A with C's IP address (or domain name).
- 3 Client device A then sends the call invitation to client device C.

**Figure 99** SIP Redirect Server

#### 11.2.2.4 SIP Register Server

A SIP register server maintains a database of SIP identity-to-IP address (or domain name) mapping. The register server checks your user name and password when you register.

#### 11.2.2.5 SIP Registration

Each ZyXEL Device is an individual SIP User Agent (UA). To provide voice service, it has a public IP address for SIP and RTP protocols to communicate with other servers.

A SIP user agent has to register with the SIP registrar and must provide information about the users it represents, as well as its current IP address (for the routing of incoming SIP requests). After successful registration, the SIP server knows that the users (identified by their dedicated SIP URIs; see [Section 11.2.1.2 on page 170](#)) are represented by the UA, and knows the IP address to which the SIP requests and responses should be sent.

Registration is initiated by the User Agent Client (UAC) running in the VoIP gateway (the ZyXEL Device). The gateway must be configured with information letting it know where to send the REGISTER message, as well as the relevant user and authorization data.

A SIP registration has a limited lifespan. The User Agent Client must renew its registration within this lifespan. If it does not do so, the registration data will be deleted from the SIP registrar's database and the connection broken.

The ZyXEL Device attempts to register all enabled subscriber ports when it is switched on. When you enable a subscriber port that was previously disabled, the ZyXEL Device attempts to register the port immediately.

#### 11.2.2.6 Authorization Requirements

SIP registrations (and subsequent SIP requests) require a username and password for authorization. These credentials are validated via a challenge / response system using the HTTP digest mechanism (as detailed in RFC3261, "SIP: Session Initiation Protocol").

### 11.2.3 RTP

When you make a VoIP call using SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

### 11.2.4 Pulse Code Modulation

Pulse Code Modulation (PCM) measures analog signal amplitudes at regular time intervals and converts them into bits.

### 11.2.5 SIP Call Progression

The following figure displays the basic steps in the setup and tear down of a SIP call. A calls B.

**Table 58** SIP Call Progression

A		B
1. INVITE	→	
	←	2. Ringing
	←	3. OK
4. ACK	→	
		5. Dialogue (voice traffic)
6. BYE	→	
	←	7. OK

A sends a SIP INVITE request to B. This message is an invitation for B to participate in a SIP telephone call.

- 4 B sends a response indicating that the telephone is ringing.
- 5 B sends an OK response after the call is answered.
- 6 A then sends an ACK message to acknowledge that B has answered the call.
- 7 Now A and B exchange voice media (talk).
- 8 After talking, A hangs up and sends a BYE request.
- 9 B replies with an OK response confirming receipt of the BYE request and the call is terminated.

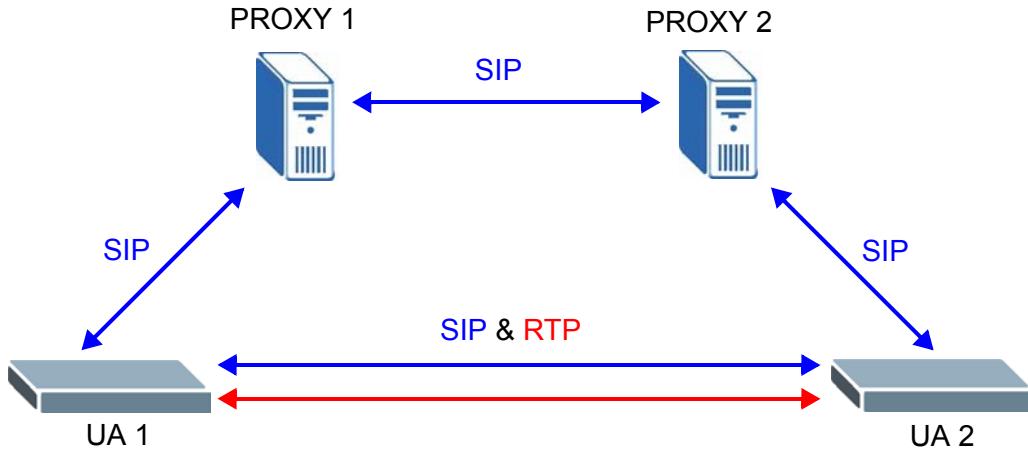
### 11.2.6 SIP Call Progression Through Proxies

Usually, the SIP UAC sets up a phonecall by sending a request to the SIP proxy server. Then, the proxy server looks up the destination to which the call should be forwarded (according to the URI requested by the SIP UAC). The request may be forwarded to more than one proxy server before arriving at its destination.

The response to the request goes to all the proxy servers through which the request passed, in reverse sequence. Once the session is set up, session traffic is sent between the UAs directly, bypassing all the proxy servers in between.

The following figure shows the SIP and session traffic flow between the user agents (UA 1 and UA 2) and the proxy servers (this example shows two proxy servers, PROXY 1 and PROXY 2).

**Figure 100** SIP Call Through Proxy Servers



The following table shows the SIP call progression.

**Table 59** SIP Call Progression

UA 1		PROXY 1		PROXY 2		UA 2
Invite	→					
		Invite	→			
		←	100 Trying			
				Invite	→	
				←	100 Trying	
					180 Ringing	←
					←	180 Ringing
					180 Ringing	←
					200 OK	←
					200 OK	→
ACK	→					
RTP	→					RTP
						BYE
					200 OK	→

- 1 User Agent 1 sends a SIP INVITE request to Proxy 1. This message is an invitation to User Agent 2 to participate in a SIP telephone call. Proxy 1 sends a response indicating that it is trying to complete the request.
- 2 Proxy 1 sends a SIP INVITE request to Proxy 2. Proxy 2 sends a response indicating that it is trying to complete the request.
- 3 Proxy 2 sends a SIP INVITE request to User Agent 2.
- 4 User Agent 2 sends a response back to Proxy 2 indicating that the phone is ringing. The response is relayed back to User Agent 1 via Proxy 1.

- 5** **User Agent 2** sends an OK response to **Proxy 2** after the call is answered. This is also relayed back to **User Agent 1** via **Proxy 1**.
- 6** **User Agent 1** and **User Agent 2** exchange RTP packets containing voice data directly, without involving the proxies.
- 7** When **User Agent 2** hangs up, he sends a BYE request.
- 8** **User Agent 1** replies with an OK response confirming receipt of the BYE request, and the call is terminated.

### 11.2.7 Voice Coding

A codec (coder/decoder) codes analog voice signals into digital signals and decodes the digital signals back into analog voice signals. The ZyXEL Device supports the following codecs.

- G.711 is a Pulse Code Modulation (PCM) waveform codec. PCM measures analog signal amplitudes at regular time intervals and converts them into digital samples. G.711 provides very good sound quality but requires 64 kbps of bandwidth.
- G.726 is an Adaptive Differential PCM (ADPCM) waveform codec that uses a lower bitrate than standard PCM conversion. ADPCM converts analog audio into digital signals based on the difference between each audio sample and a prediction based on previous samples. The more similar the audio sample is to the prediction, the less space needed to describe it. G.726 operates at 16, 24, 32 or 40 kbps.
- G.729 is an Analysis-by-Synthesis (AbS) hybrid waveform codec that uses a filter based on information about how the human vocal tract produces sounds. G.729 provides good sound quality and reduces the required bandwidth to 8 kbps.

### 11.2.8 PSTN Call Setup Signaling

Dual-Tone MultiFrequency (DTMF) signaling uses pairs of frequencies (one lower frequency and one higher frequency) to set up calls. It is also known as Touch Tone®. Each of the keys on a DTMF telephone corresponds to a different pair of frequencies.

Pulse dialing sends a series of clicks to the local phone office in order to dial numbers.<sup>4</sup>

### 11.2.9 MWI (Message Waiting Indication)

Enable Message Waiting Indication (MWI) enables your phone to give you a message-waiting (beeping) dial tone when you have a voice message(s). Your VoIP service provider must have a messaging system that sends message waiting status SIP packets as defined in RFC 3842.

---

4. The ZyXEL Device does not support pulse dialing at the time of writing.

## 11.2.10 Custom Tones (IVR)

IVR (Interactive Voice Response) is a feature that allows you to use your telephone to interact with the ZyXEL Device. The ZyXEL Device allows you to record custom tones for the **Caller Ringing Tone** and **On Hold Tone** functions. The same recordings apply to both the caller ringing and on hold tones.

**Table 60** Custom Tones Details

LABEL	DESCRIPTION
Total Time for All Tones	128 seconds for all custom tones combined
Time per Individual Tone	20 seconds
Total Number of Tones Recordable	8 You can record up to 8 different custom tones but the total time must be 128 seconds or less.

### 11.2.10.1 Recording Custom Tones

Use the following steps if you would like to create new tones or change your tones:

- 1 Pick up the phone and press “\*\*\*\*\*” on your phone’s keypad and wait for the message that says you are in the configuration menu.
- 2 Press a number from 1101~1108 on your phone followed by the “#” key.
- 3 Play your desired music or voice recording into the receiver’s mouthpiece. Press the “#” key.
- 4 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

### 11.2.10.2 Listening to Custom Tones

Do the following to listen to a custom tone:

- 1 Pick up the phone and press “\*\*\*\*\*” on your phone’s keypad and wait for the message that says you are in the configuration menu.
- 2 Press a number from 1201~1208 followed by the “#” key to listen to the tone.
- 3 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

### 11.2.10.3 Deleting Custom Tones

Do the following to delete a custom tone:

- 1 Pick up the phone and press “\*\*\*\*\*” on your phone’s keypad and wait for the message that says you are in the configuration menu.
- 2 Press a number from 1301~1308 followed by the “#” key to delete the tone of your choice. Press 14 followed by the “#” key if you wish to clear all your custom tones.

You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

## 11.3 Quality of Service (QoS)

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to provide bandwidth for real-time multimedia applications.

### 11.3.1 Type Of Service (ToS)

Network traffic can be classified by setting the ToS (Type Of Service) values at the data source (for example, at the ZyXEL Device) so a server can decide the best method of delivery, that is the least cost, fastest route and so on.

### 11.3.2 DiffServ

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.<sup>5</sup>

#### 11.3.2.1 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

**Figure 101** DiffServ: Differentiated Service Field

DSCP (6-bit)	Unused (2-bit)
-----------------	-------------------

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

### 11.3.3 VLAN

Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. Only stations within the same group can communicate with each other.

Your ZyXEL Device can add IEEE 802.1Q VLAN ID tags to voice frames that it sends to the network. This allows the ZyXEL Device to communicate with a SIP server that is a member of the same VLAN group. Some ISPs use the VLAN tag to identify voice traffic and give it priority over other traffic.

---

5. The ZyXEL Device does not support DiffServ at the time of writing.

## 11.4 SIP Settings Screen

The ZyXEL Device uses a SIP account to make outgoing VoIP calls and check if an incoming call's destination number matches your SIP account's SIP number. In order to make or receive a VoIP call, you need to enable and configure a SIP account, and map it to a phone port. The SIP account contains information that allows your ZyXEL Device to connect to your VoIP service provider.

If you want to make only peer-to-peer VoIP calls, there is no VoIP service provider involved, so the SIP account information does not have to match a real VoIP service provider's SIP account. You can make up the SIP numbers. However, you should still activate a SIP account and configure its number and map it to a phone port, so that the person you call knows what SIP number you are using and the ZyXEL Device knows to which phone port it should forward an incoming VoIP call. You must use speed dial to make peer-to-peer VoIP calls.

See [Section 11.8.2 on page 185](#) for how to map a SIP account to a phone port.

Use this screen to maintain basic information about each SIP account. You can also enable and disable each SIP account. To access this screen, click **VoIP > SIP > SIP Settings**.

**Figure 102** SIP > SIP Settings

LABEL	DESCRIPTION
SIP Account	Select the SIP account you want to see in this screen. If you change this field, the screen automatically refreshes.
SIP Settings	

Each field is described in the following table.

**Table 61** SIP > SIP Settings

LABEL	DESCRIPTION
SIP Account	Select the SIP account you want to see in this screen. If you change this field, the screen automatically refreshes.
SIP Settings	

**Table 61** SIP > SIP Settings

LABEL	DESCRIPTION
Active SIP Account	Select this if you want the ZyXEL Device to use this account. Clear it if you do not want the ZyXEL Device to use this account.
Number	Enter your SIP number. In the full SIP URI, this is the part before the @ symbol. You can use up to 127 printable ASCII characters.
SIP Local Port	Enter the ZyXEL Device's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
SIP Server Address	Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 95 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server.
SIP Server Port	Enter the SIP server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
REGISTER Server Address	Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the <b>SIP Server Address</b> field. You can use up to 95 printable ASCII characters.
REGISTER Server Port	Enter the SIP register server's listening port number, if your VoIP service provider gave you one. Otherwise, enter the same port number you entered in the <b>SIP Server Port</b> field.
SIP Service Domain	Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 127 printable ASCII Extended set characters.
Send Caller ID	Select this if you want to send identification when you make VoIP phone calls. Clear this if you do not want to send identification.
Authentication	
User Name	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII characters.
Password	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII Extended set characters.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.
Advanced Setup	Click this to edit the advanced settings for this SIP account. The <b>Advanced SIP Setup</b> screen appears.

## 11.5 Advanced SIP Setup Screen

Click **VoIP > SIP > SIP Settings** to open the **SIP Settings** screen. Select a SIP account and click **Advanced Setup** to open the **Advanced SIP Setup** screen. Use this screen to maintain advanced settings for each SIP account.

**Figure 103** VoIP > SIP Settings > Advanced

SIP Account :SIP1

**SIP Server Settings**

URL Type	SIP
Expiration Duration	3600 (20-65535) sec
Register Re-send timer	180 (1-65535) sec
Session Expires	300 (30-3600) sec
Min-SE	180 (20-1800) sec

**RTP Port Range**

Start Port	40000 (1025-65535)
End Port	65535 (1025-65535)

**Voice Compression**

Primary Compression Type	G.711A
Secondary Compression Type	G.729
Third Compression Type	G.711u
DTMF Mode	RFC 2833

**Outbound Proxy**

<input type="checkbox"/> Enable	
Server Address	
Server Port	0 (1025-65535)

**MWI (Message Waiting Indication)**

<input type="checkbox"/> Enable	
Expiration Time	120 (1-65535) sec

**Call Forward**

Call Forward Table	Table 1
--------------------	---------

**Caller Ringing**

<input type="checkbox"/> Enable	
Caller Ringing Tone	Default

**On Hold**

<input type="checkbox"/> Enable	
On Hold Tone	Default

**Back**    **Apply**    **Cancel**

Each field is described in the following table.

**Table 62** VoIP > SIP Settings > Advanced

LABEL	DESCRIPTION
SIP Account	This field displays the SIP account you see in this screen.
SIP Server Settings	

**Table 62** VoIP > SIP Settings > Advanced

LABEL	DESCRIPTION
URL Type	Select whether or not to include the SIP service domain name when the ZyXEL Device sends the SIP number. <b>SIP</b> - include the SIP service domain name. <b>TEL</b> - do not include the SIP service domain name.
Expiration Duration	Enter the number of seconds your SIP account is registered with the SIP register server before it is deleted. The ZyXEL Device automatically tries to re-register your SIP account when one-half of this time has passed. (The SIP register server might have a different expiration.)
Register Re-send timer	Enter the number of seconds the ZyXEL Device waits before it tries again to register the SIP account, if the first try failed or if there is no response.
Session Expires	Enter the number of seconds the ZyXEL Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session.
Min-SE	Enter the minimum number of seconds the ZyXEL Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session. When two SIP devices start a SIP session, they must agree on an expiration time for idle sessions. This field is the shortest expiration time that the ZyXEL Device accepts.
RTP Port Range	
Start Port End Port	Enter the listening port number(s) for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values. To enter one port number, enter the port number in the <b>Start Port</b> and <b>End Port</b> fields. To enter a range of ports, <ul style="list-style-type: none"><li>• enter the port number at the beginning of the range in the <b>Start Port</b> field.</li><li>• enter the port number at the end of the range in the <b>End Port</b> field.</li></ul>
Voice Compression	Select the type of voice coder/decoder (codec) that you want the ZyXEL Device to use. G.711 provides higher voice quality but requires more bandwidth (64 kbps). <ul style="list-style-type: none"><li>• <b>G.711A</b> is typically used in Europe.</li><li>• <b>G.711u</b> is typically used in North America and Japan.</li></ul> <b>G.726</b> operates at <b>16, 24, 32 or 40</b> kbps. By contrast, <b>G.729</b> only requires 8 kbps. The ZyXEL Device must use the same codec as the peer. When two SIP devices start a SIP session, they must agree on a codec.
Primary Compression Type	Select the ZyXEL Device's first choice for voice coder/decoder.
Secondary Compression Type	Select the ZyXEL Device's second choice for voice coder/decoder. Select <b>None</b> if you only want the ZyXEL Device to accept the first choice.
Third Compression Type	Select the ZyXEL Device's third choice for voice coder/decoder. Select <b>None</b> if you only want the ZyXEL Device to accept the first or second choice.
DTMF Mode	Control how the ZyXEL Device handles the tones that your telephone makes when you push its buttons. You should use the same mode your VoIP service provider uses. <b>RFC 2833</b> - send the DTMF tones in RTP packets. <b>PCM</b> - send the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729 and G.726) can distort the tones. <b>SIP INFO</b> - send the DTMF tones in SIP messages.
Outbound Proxy	

**Table 62** VoIP > SIP Settings > Advanced

LABEL	DESCRIPTION
Enable	Select this if your VoIP service provider has a SIP outbound server to handle voice calls. This allows the ZyXEL Device to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off any SIP ALG on a NAT router in front of the ZyXEL Device to keep it from retranslating the IP address (since this is already handled by the outbound proxy server).
Server Address	Enter the IP address or domain name of the SIP outbound proxy server.
Server Port	Enter the SIP outbound proxy server's listening port, if your VoIP service provider gave you one. Otherwise, keep the default value.
MWI (Message Waiting Indication)	
Enable	Select this if you want to hear a waiting (beeping) dial tone on your phone when you have at least one voice message. Your VoIP service provider must support this feature.
Expiration Time	Keep the default value for this field, unless your VoIP service provider tells you to change it. Enter the number of seconds the SIP server should provide the message waiting service each time the ZyXEL Device subscribes to the service. Before this time passes, the ZyXEL Device automatically subscribes again.
Call Forward	
Call Forward Table	Select which call forwarding table you want the ZyXEL Device to use for incoming calls. You set up these tables in <b>VoIP &gt; Phone Book &gt; Incoming Call Policy</b> .
Caller Ringing	
Enable	Select the check box if you want to specify what tone people hear when they call you. The ZyXEL Device provides a default tone, but you can add additional tones using IVR. See <a href="#">Section 11.2.10 on page 176</a> for more information.
Caller Ringing Tone	Select the tone you want people to hear when they call you. You should set up these tones using IVR first. See <a href="#">Section 11.2.10 on page 176</a> for more information.
On Hold	
Enable	Select the check box if you want to specify what tone people hear when you put them on hold. The ZyXEL Device provides a default tone, but you can add additional tones using IVR. See <a href="#">Section 11.2.10 on page 176</a> for more information.
On Hold Tone	Select the tone you want people to hear when you put them on hold. You should setup these tones using IVR first. See <a href="#">Section 11.2.10 on page 176</a> for more information.
Back	Click this to return to the <b>SIP Settings</b> screen without saving your changes.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

## 11.6 SIP QoS Screen

Use this screen to maintain ToS and VLAN settings for the ZyXEL Device. To access this screen, click **VoIP > SIP > QoS**.

**Figure 104** SIP > QoS

SIP Settings    **QoS**

**TOS**

SIP TOS Priority Setting:  (0~255)  
RTP TOS Priority Setting:  (0~255)

**VLAN Tagging**

Voice VLAN ID:  (0~4095)

**Buttons:** Apply    Reset

Each field is described in the following table.

**Table 63** SIP > QoS

LABEL	DESCRIPTION
SIP TOS Priority Setting	Enter the priority for SIP voice transmissions. The ZyXEL Device creates Type of Service priority tags with this priority to voice traffic that it transmits.
RTP TOS Priority Setting	Enter the priority for RTP voice transmissions. The ZyXEL Device creates Type of Service priority tags with this priority to RTP traffic that it transmits.
Voice VLAN ID	Select this if the ZyXEL Device has to be a member of a VLAN to communicate with the SIP server. Ask your network administrator, if you are not sure. Enter the VLAN ID provided by your network administrator in the field on the right. Your LAN and gateway must be configured to use VLAN tags. Otherwise, clear this field.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

## 11.7 Phone

You can configure the volume, echo cancellation and VAD settings for each individual phone port on the ZyXEL Device. You can also select which SIP account to use for making outgoing calls.

### 11.7.1 PSTN Line

With the PSTN line you can make and receive regular PSTN phone calls. Use a prefix number to make a regular call. When the device does not have power, you can make regular calls without dialing a prefix number.



When the ZyXEL Device does not have power, only the phone connected to the **PHONE 1** port can be used for making calls. Ensure you know which phone this is, so that in case of emergency you can make outgoing calls.

You can also use the **PSTN Line** screen to specify phone numbers that should always use the regular phone service (without having to dial a prefix number). Do this for emergency numbers (like those for contacting police, fire or emergency medical services).

### 11.7.2 ISDN Line

With an ISDN line you can make and receive regular ISDN phone calls. Use a prefix number to make a regular call.

You can also use the **ISDN Line** screen to specify phone numbers that should always use the regular phone service (without having to dial a prefix number). Do this for emergency numbers (like those for contacting police, fire or emergency medical services).

### 11.7.3 Voice Activity Detection/Silence Suppression

Voice Activity Detection (VAD) detects whether or not speech is present. This lets the ZyXEL Device reduce the bandwidth that a call uses by not transmitting “silent packets” when you are not speaking.

### 11.7.4 Comfort Noise Generation

When using VAD, the ZyXEL Device generates comfort noise when the other party is not speaking. The comfort noise lets you know that the line is still connected as total silence could easily be mistaken for a lost connection.

### 11.7.5 Echo Cancellation

G.168 is an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.

## 11.8 Analog Phone

This screen allows you to configure the **PHONE 1** and **PHONE 2** ports on the ZyXEL Device. These ports are for connecting analog phones to the ZyXEL Device. You can configure different settings for each **PHONE** port.



---

If you connect more than one analog phone to a single **PHONE** port, the settings you configure on the port apply to all phones connected to the port.

---

### 11.8.1 PHONE Port Call Types

You can use the analog phones connected to the ZyXEL Device’s **PHONE 1** and **PHONE 2** ports to make and receive three kinds of call:

- Internet phone calls (Voice over IP or VoIP). These calls are made and received using the Internet connection on your ZyXEL Device. You need to configure a SIP account (see [Section 11.4 on page 178](#)) before making Internet phone calls.
- Analog phone calls. These calls are made and received using a PSTN (Public Switched Telephone Network) line connected to the **PSTN/ISDN** port on the ZyXEL Device.
- ISDN (Integrated Services Digital Network) phone calls. These calls are made and received using an ISDN line connected to the **PSTN/ISDN** port on the ZyXEL Device.



If you use an analog phone to make and receive calls over the ISDN line, not all ISDN features may be available. Contact your ISDN service provider for details.

#### 11.8.1.1 Analog Phones and Multiple Subscriber Numbers

Multiple Subscriber Numbers (MSNs) allow you to use more than one phone number on a single ISDN phone line (see [Section 11.23.1 on page 208](#)). If you have MSNs from your ISDN service provider, you can use the **Analog Phone** screen to have the phone(s) connected to the analog **PHONE** ports make and receive ISDN calls using one or more MSNs. You must first configure the MSNs you want to use in the **VoIP > Fixed Line Numbers** screen (see [Section 11.23 on page 208](#)).

#### 11.8.2 Configuring the Analog Phone Screen

Use the **Analog Phone** screen to do the following.

- Configure which SIP accounts each **PHONE** port uses to make and receive VoIP calls.
- Configure whether phones connected to each **PHONE** port can make and receive analog and ISDN calls.



Phones connected to the **PHONE** ports make outgoing calls using a SIP account by default. You must enter a prefix number in your phone's keypad if you want to make analog or ISDN calls. Use the **VoIP > PSTN Line** screen to configure the prefix number for analog calls (see [Section 11.21 on page 206](#)) and use the **VoIP > ISDN Line** screen to configure the prefix number for ISDN calls (see [Section 11.22 on page 207](#)).

Click **VoIP > Phone > Analog Phone**. The following screen displays.

**Figure 105** Phone > Analog Phone

Each field is described in the following table.

**Table 64** Phone > Analog Phone

LABEL	DESCRIPTION
Phone Port Settings	Select the <b>PHONE</b> port you want to see in this screen. If you change this field, the screen automatically refreshes.
Outgoing Call Use	Use this section to configure the type of calls you can make from a phone connected to this <b>PHONE</b> port.
SIP Account	You must configure a SIP account in the <b>VoIP &gt; SIP</b> screen before you can make VoIP phone calls. Select which SIP account you want to use for outgoing calls from phones connected to this <b>PHONE</b> port.
PSTN Line	Select this to allow outgoing calls from phones connected to this phone port to use the analog (PSTN) phone line. You need to enter the prefix number you configure in the <b>VoIP &gt; PSTN Line</b> screen when you want to make an analog call.
ISDN Line	Select this to allow outgoing calls from phones connected to this port to use the digital (ISDN) phone line. You need to enter the prefix number you configure in the <b>VoIP &gt; ISDN Line</b> screen when you want to make an ISDN call.
MSN	When you select a number in this field, outgoing ISDN calls from phones connected to this <b>PHONE</b> port use the corresponding MSN. Alternatively, leave this field blank if you do not use an MSN service or do not want to use MSNs for outgoing calls.  <b>Note:</b> The <b>MSN</b> number refers to the MSN mapping entries you configure in the <b>VoIP &gt; Fixed Line Numbers</b> screen. Configure these entries first.
Incoming Call apply to	Use this section to configure the type of calls you can receive on a phone connected to this <b>PHONE</b> port.

**Table 64** Phone > Analog Phone

LABEL	DESCRIPTION
SIP1 ~ SIP10	You must configure a SIP account in the <b>VoIP &gt; SIP</b> screen before you can receive VoIP phone calls. Select which SIP accounts you want to receive phone calls from on this phone port. If you select more than one source for incoming calls, there is no way to distinguish between them when you receive phone calls.
PSTN Line	Select this if you want to receive phone calls from the PSTN line (that do not use the Internet) on this phone port. If you select more than one source for incoming calls, there is no way to distinguish between them when you receive phone calls.
ISDN Line	Select this if you want to receive phone calls from the ISDN line (that do not use the Internet) on this phone port. If you select more than one source for incoming calls, there is no way to distinguish between them when you receive phone calls.
MSN	<p>Select the MSNs you want the phone(s) connected to this phone port to receive. When there is an incoming call with the corresponding MSN, the phones connected to this port ring. Leave these fields blank if you do not use an MSN service.</p> <p>If you select more than one source for incoming calls, there is no way to distinguish between them when you receive phone calls.</p> <p><b>Note:</b> The number in the <b>MSN</b> field refers to the MSN mapping entries you configure in the <b>VoIP &gt; Fixed Line Numbers</b> screen. Configure these entries first.</p> <p><b>Note:</b> If you use an MSN service but do NOT configure MSNs in this screen, when you select <b>ISDN Line</b> the phone(s) attached to this port can receive calls that use any MSN.</p>
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.
Advanced Setup	Click this to edit the advanced settings for this phone port. The <b>Advanced Analog Phone Setup</b> screen appears.

## 11.9 Advanced Analog Phone Setup Screen

Use this screen to edit advanced settings for each phone port. To access this screen, click **Advanced Setup** in **VoIP > Phone > Analog Phone**.

**Figure 106** Phone > Analog Phone > Advanced

Analog Phone 1

**Voice Volume Control**

Speaking Volume: -1(Min.)  
Listening Volume: -1(Min.)

**Echo Cancellation**

G.168 Active

**Fax Option**

G.711 Fax Passthrough       T.38 Fax Relay

**Dialing Interval Select**

Dialing Interval Select: 5

**Voice Active Detector**

VAD Support

**Auto Dial**

Auto Dial Active  
Auto Dial Phone Number: [ ]

Back    Apply    Cancel

Each field is described in the following table.

**Table 65** Phone > Analog Phone > Advanced

LABEL	DESCRIPTION
Analog Phone	This field displays the number of the analog phone you are currently configuring.
Voice Volume Control	
Speaking Volume	Enter the loudness that the ZyXEL Device uses for speech that it sends to the peer device. -1 is the quietest, and 1 is the loudest.
Listening Volume	Enter the loudness that the ZyXEL Device uses for speech that it receives from the peer device. -1 is the quietest, and 1 is the loudest.
Echo Cancellation	
G.168 Active	Select this if you want to eliminate the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
Fax Option	This field controls how the ZyXEL Device handles fax messages.
G.711 Fax Passthrough	Select this if the ZyXEL Device should use G.711 to send fax messages. The peer devices must also use G.711.
T.38 Fax Relay	Select this if the ZyXEL Device should send fax messages as UDP or TCP/IP packets through IP networks. This provides better quality, but it may have interoperability problems. The peer devices must also use T.38.
Dialing Interval Select	

**Table 65** Phone > Analog Phone > Advanced

LABEL	DESCRIPTION
Dialing Interval Select	Enter the number of seconds the ZyXEL Device should wait after you stop dialing numbers before it makes the phone call. The value depends on how quickly you dial phone numbers. If you select <b>Active Immediate Dial</b> in <b>VoIP &gt; Phone &gt; Common</b> , you can press the pound key (#) to tell the ZyXEL Device to make the phone call immediately, regardless of this setting.
Voice Active Detector	
Active VAD	Select this if the ZyXEL Device should stop transmitting when you are not speaking. This reduces the bandwidth the ZyXEL Device uses.
Auto Dial	
Active Auto Dial	Select this if you want the ZyXEL Device to automatically dial the phone number you enter in the <b>Auto Dial Phone Number</b> field as soon as you take the phone off the hook.
Auto Dial Phone Number	If you select <b>Active Auto Dial</b> , enter the phone number you want the ZyXEL Device to automatically dial in this field.
Back	Click this to return to the <b>Analog Phone</b> screen without saving your changes.
Apply	Click this to save your changes.
Cancel	Click this to set every field in this screen to its last-saved value.

## 11.10 ISDN Phone

This screen allows you to configure the outgoing and incoming call settings for ISDN phones connected to the ZyXEL Device via the **ISDN PHONE** port. At the time of writing, the ZyXEL Device can connect up to eight ISDN phones to the **ISDN PHONE** port. An ISDN phone can have more than one MSN (Multiple Subscriber Number). Each MSN can have different settings in the **ISDN Phone** screen.




---

If you want to use ISDN phones connected to the ZyXEL Device, you must configure your ISDN phones to use the same MSNs.

---

### 11.10.1 ISDN Phone Port Call Types

You can use ISDN phones connected to the ZyXEL Device's **ISDN PHONE** port to make and receive three kinds of call:

- Internet phone calls (Voice over IP or VoIP). These calls are made and received using the Internet connection on your ZyXEL Device. You need to configure a SIP account (see [Section 11.4 on page 178](#)) before making Internet phone calls.
- Analog phone calls. These calls are made and received using a PSTN (Public Switched Telephone Network) line connected to the **PSTN/ISDN** port on the ZyXEL Device.
- ISDN (Integrated Services Digital Network) phone calls. These calls are made and received using an ISDN line connected to the **PSTN/ISDN** port on the ZyXEL Device.

## 11.10.2 Configuring the ISDN Phone Screen

Use the **ISDN Phone** screen to do the following.

- Configure which SIP account ISDN phones use to make VoIP calls.
- Configure which SIP account ISDN phones use for incoming calls.
- Configure whether ISDN phones can receive PSTN calls.

Click **VoIP > Phone > ISDN Phone**. The following screen displays.

**Figure 107** Phone > ISDN Phone

Each field is described in the following table.

**Table 66** Phone > ISDN Phone

LABEL	DESCRIPTION
ISDN Phone Port Settings	Select the MSN you want to configure. If you change this field, the screen automatically refreshes. If you configured the extension number of MSNs in the <b>VoIP &gt; Ext. Table</b> screen, the extension number of the corresponding MSN displays.  Note: The extension number refers to the MSN mapping entries you configure in the <b>VoIP &gt; Phone &gt; Ext. Table</b> screen. Configure these first.
Outgoing Call Use	Use this section to configure the SIP account you want to use for outgoing calls with the MSN you selected.
SIP Account	You must configure a SIP account in the <b>VoIP &gt; SIP</b> screen before you can make VoIP phone calls. Select which SIP account you want to use for outgoing calls with the MSN you selected.
Incoming Call apply to	Use this section to configure the SIP account you want to use for incoming calls, and whether or not you want to receive incoming PSTN calls with the MSN you selected.
SIP Account	You must configure a SIP account in the <b>VoIP &gt; SIP</b> screen before you can receive VoIP phone calls. Select which SIP account you want to receive phone calls from on this phone port. If you select more than one source for incoming calls, there is no way to distinguish between them when you receive phone calls.
PSTN Line	Select this if you want to receive phone calls from the PSTN line on the phone port. If you select more than one source for incoming calls, there is no way to distinguish between them when you receive phone calls.
Apply	Click this to save your changes.
Cancel	Click this to set every field in this screen to its last-saved value.

## 11.11 Common Phone Settings Screen

Use this screen to activate and deactivate immediate dialing and set up call fallback. To access this screen, click **VoIP > Phone > Common**.

**Figure 108** Phone > Common



Each field is described in the following table.

**Table 67** Phone > Common

LABEL	DESCRIPTION
Immediate Dial	
Active Immediate Dial	Select this if you want to use the pound key (#) to tell the ZyXEL Device to make the phone call immediately, instead of waiting the number of seconds you selected in the <b>Dialing Interval Select</b> in <b>VoIP &gt; Phone &gt; Analog Phone</b> . If you select this, dial the phone number, and then press the pound key. The ZyXEL Device makes the call immediately, instead of waiting. You can still wait, if you want.
Call Fallback	
Force to PSTN if SIP unregistered	Select this to have the ZyXEL Device redirect outgoing calls to the PSTN connection if there are no SIP accounts registered on the ZyXEL Device. When you try to make a SIP call, but no SIP account is registered, the ZyXEL Device uses the phone line connected to the PSTN port to make the call.
Force to SIP if PSTN unplugged	Select this to have the ZyXEL Device redirect outgoing calls to the registered SIP account if the ZyXEL Device is not connected to the PSTN network. When you try to make a PSTN call, but the PSTN port on the ZyXEL Device is unplugged, the ZyXEL Device uses the phone port's registered SIP account to make the call.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

## 11.12 Ext. Table

You can assign extension numbers to phones connected to the ZyXEL Device, and make internal calls between these phones. For information on making internal calls, refer to [Section 13.3 on page 227](#).

For the **PHONE 1** and **PHONE 2** ports, an extension number is composed of a group number and a sub number. If group number is not enabled, the extension number is simply the sub number. You can assign a group number to the two phone ports. When you dial a group number, all phones belonging to that group ring.

The MSNs you configure are used by the ISDN phone(s) connected to the ISDN port. You must also configure your ISDN phone(s) to use these MSNs. You can use the MSN to call an ISDN phone from another phone connected to the ZyXEL Device.



If an ISDN phone already has a MSN configured (for making and receiving ISDN calls), do not change it; otherwise ISDN calls may not work.

Use the **Ext. Table** screen to configure the extension number of the **PHONE 1** and **PHONE 2** ports, and ISDN phones connected to the **ISDN PHONE** port on the ZyXEL Device. To access this screen, click **VoIP > Phone > Ext. Table**.



Make sure each **Extension Number** you configure in the **Ext. Table** screen is unique.

**Figure 109** VoIP > Phone > Ext. Table

Analog Phone	ISDN Phone	Common	<b>Ext. Table</b>	Region																											
<input type="checkbox"/> Enable Group Number																															
<b>Phone</b> <table border="1"> <thead> <tr> <th>#</th> <th>Group Number</th> <th>Sub Number</th> <th>Extension Number</th> <th>Advanced</th> </tr> </thead> <tbody> <tr> <td>Phone 1</td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td></td> </tr> <tr> <td>Phone 2</td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td></td> </tr> </tbody> </table>					#	Group Number	Sub Number	Extension Number	Advanced	Phone 1	<input type="text"/>	<input type="text"/>	<input type="text"/>		Phone 2	<input type="text"/>	<input type="text"/>	<input type="text"/>													
#	Group Number	Sub Number	Extension Number	Advanced																											
Phone 1	<input type="text"/>	<input type="text"/>	<input type="text"/>																												
Phone 2	<input type="text"/>	<input type="text"/>	<input type="text"/>																												
<b>ISDN Phone</b> <table border="1"> <thead> <tr> <th>#</th> <th>Sub Number</th> <th>Extension Number</th> </tr> </thead> <tbody> <tr> <td>MSN 1</td> <td><input type="text"/></td> <td></td> </tr> <tr> <td>MSN 2</td> <td><input type="text"/></td> <td></td> </tr> <tr> <td>MSN 3</td> <td><input type="text"/></td> <td></td> </tr> <tr> <td>MSN 4</td> <td><input type="text"/></td> <td></td> </tr> <tr> <td>MSN 5</td> <td><input type="text"/></td> <td></td> </tr> <tr> <td>MSN 6</td> <td><input type="text"/></td> <td></td> </tr> <tr> <td>MSN 7</td> <td><input type="text"/></td> <td></td> </tr> <tr> <td>MSN 8</td> <td><input type="text"/></td> <td></td> </tr> </tbody> </table>					#	Sub Number	Extension Number	MSN 1	<input type="text"/>		MSN 2	<input type="text"/>		MSN 3	<input type="text"/>		MSN 4	<input type="text"/>		MSN 5	<input type="text"/>		MSN 6	<input type="text"/>		MSN 7	<input type="text"/>		MSN 8	<input type="text"/>	
#	Sub Number	Extension Number																													
MSN 1	<input type="text"/>																														
MSN 2	<input type="text"/>																														
MSN 3	<input type="text"/>																														
MSN 4	<input type="text"/>																														
MSN 5	<input type="text"/>																														
MSN 6	<input type="text"/>																														
MSN 7	<input type="text"/>																														
MSN 8	<input type="text"/>																														
<input type="button" value="Apply"/> <input type="button" value="Reset"/>																															

Each field is described in the following table.

**Table 68** VoIP > Phone > Ext. Table

LABEL	DESCRIPTION
Enable Group Number	Select this if you want to use the group number for <b>PHONE 1</b> and <b>PHONE 2</b> ports.
Phone	
#	This is the phone port number.
Group Number	Enter a group number for this phone port. The maximum length of a group number is four digits. This is only available when you select <b>Enable Group Number</b> . For example, you can assign the <b>Phone 1</b> and <b>Phone 2</b> ports the group number "5". When you dial "5", all the phones connected to both <b>Phone</b> ports ring.
Sub Number	Enter a sub number for this phone. The maximum length of a sub number is four digits. When the <b>Enable Group Number</b> is not selected, the extension number is simply the sub number.
Extension Number	This read-only field displays the extension number, which is a combination of the <b>Group Number</b> and the <b>Sub Number</b> . When you change a group number or a sub number, the extension number automatically refreshes. Use the extension number to make calls between phones connected to the ZyXEL Device.
Advanced	Click the edit icon to edit advanced settings
ISDN Phone	
#	This is the MSN index number.
Sub Number	Enter a sub number for this MSN. The maximum length of a sub number is four digits.  Note: If an ISDN phone already has MSNs configured for ISDN calls, use the existing MSNs.
Extension Number	This read-only field displays the extension number. When you change the <b>Sub number</b> of an MSN, the extension number automatically refreshes. When you call an MSN's extension number, all phones configured to use that MSN ring.
Apply	Click this to save your changes.
Cancel	Click this to set every field in this screen to its last-saved value.

## 11.13 Advanced Ext. Table Setup Screen

You can create call-forwarding rules for internal calls. To access this screen, click **Advanced** in a phone extension entry in the **VoIP > Phone > Ext. Table** screen.

**Figure 110** VoIP > Phone > Ext. Table > Advanced

Forward to Number Setup

Unconditional Forward to Number

Busy Forward to Number

No Answer Forward to Number

No Answer Waiting Time  (Second)

**Back** **Apply** **Reset**

Each field is described in the following table.

**Table 69** VoIP > Phone > Ext. Table > Advanced

LABEL	DESCRIPTION
Forward to Number Setup	The ZyXEL Device checks these rules in the order in which they appear.
Unconditional Forward to Number	Specify the extension number to which you want the ZyXEL Device to forward all incoming internal calls.
Busy Forward to Number	Specify the extension number to which you want the ZyXEL Device to forward incoming internal calls if the phone port is busy. If you have call waiting, the incoming call is forwarded to the specified phone number if you reject or ignore the second incoming call.
No Answer Forward to Number	Specify the extension number you want the ZyXEL Device to forward incoming internal calls to if the call is unanswered. (See <b>No Answer Waiting Time</b> .)
No Answer Waiting Time	This field is used by the <b>No Answer Forward to Number</b> feature. Enter the number of seconds the ZyXEL Device should wait for you to answer an incoming internal call before it considers the call unanswered.
Back	Click this to return to the <b>Ext. Table Setup</b> Screen.
Apply	Click this to save your changes.
Cancel	Click this to set every field in this screen to its last-saved value.

## 11.14 Phone Services Overview

Supplementary services such as call hold, call waiting, call transfer, etc. are generally available from your VoIP service provider. The ZyXEL Device supports the following services:

- Call Hold
- Call Waiting
- Making a Second Call
- Call Transfer
- Call Forwarding (see [Section 11.17 on page 200](#))
- Three-Way Conference

- Internal Calls (see [Section 13.3 on page 227](#))
- Call Park and Pickup
- Do not Disturb



To take full advantage of the supplementary phone services available through the ZyXEL Device's phone ports, you may need to subscribe to the services from your VoIP service provider.

### 11.14.1 The Flash Key

Flashing means to press the hook for a short period of time (a few hundred milliseconds) before releasing it. On newer telephones, there should be a "flash" key (button) that generates the signal electronically. If the flash key is not available, you can tap (press and immediately release) the hook by hand to achieve the same effect. However, using the flash key is preferred since the timing is much more precise. With manual tapping, if the duration is too long, it may be interpreted as hanging up by the ZyXEL Device.

You can invoke all the supplementary services by using the flash key.

### 11.14.2 Europe Type Supplementary Phone Services

This section describes how to use supplementary phone services with the **Europe Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

**Table 70** European Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. Switch back to the call (if there is no second call).
Flash	0	Drop the call presently on hold or reject an incoming call which is waiting for answer.
Flash	1	Disconnect the current phone connection and answer the incoming call or resume with caller presently on hold.
Flash	2	1. Switch back and forth between two calls. 2. Put a current call on hold to answer an incoming call. 3. Separate the current three-way conference call into two individual calls (one is on-line, the other is on hold).
Flash	3	Create three-way conference connection.
Flash	*98#	Transfer the call to another phone.

#### 11.14.2.1 European Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key and then “2” to switch back and forth between caller **A** and **B** by putting either one on hold.

Press the flash key and then “0” to disconnect the call presently on hold and keep the current call on line.

Press the flash key and then “1” to disconnect the current call and resume the call on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

#### **11.14.2.2 European Call Waiting**

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to a telephone number, you will hear a call waiting tone. Take one of the following actions.

- Reject the second call.  
Press the flash key and then press “0”.
- Disconnect the first call and answer the second call.  
Either press the flash key and press “1”, or just hang up the phone and then answer the phone after it rings.
- Put the first call on hold and answer the second call.  
Press the flash key and then “2”.

#### **11.14.2.3 European Call Transfer**

Do the following to transfer an incoming call (that you have answered) to another phone.

- 1 Press the flash key to put the caller on hold.
- 2 When you hear the dial tone, dial “\*98#” followed by the number to which you want to transfer the call.
- 3 After you hear the ring signal or the second party answers it, hang up the phone.

#### **11.14.2.4 European Three-Way Conference**

Use the following steps to make three-way conference calls.

- 1 When you are on the phone talking to someone, press the flash key to put the caller on hold and get a dial tone.
- 2 Dial a phone number directly to make another call. If you want to have the call use a certain interface (SIP, PSTN or ISDN), enter the SIP, PSTN or ISDN prefix number first.
- 3 When the second call is answered, press the flash key and press “3” to create a three-way conversation.
- 4 Hang up the phone to drop the connection.
- 5 If you want to separate the activated three-way conference into two individual connections (one is on-line, the other is on hold), press the flash key and press “2”.

### **11.14.3 USA Type Supplementary Services**

This section describes how to use supplementary phone services with the **USA Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

**Table 71 USA Flash Key Commands**

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. After the second call is successful, press the flash key again to have a three-way conference call. Put a current call on hold to answer an incoming call.
Flash	*98#	Transfer the call to another phone.

#### 11.14.3.1 USA Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key to switch back and forth between caller **A** and **B** by putting either one on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

#### 11.14.3.2 USA Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to your telephone number, you will hear a call waiting tone.

Press the flash key to put the first call on hold and answer the second call.

#### 11.14.3.3 USA Call Transfer

Do the following to transfer an incoming call (that you have answered) to another phone.

- 1 Press the flash key to put the caller on hold.
- 2 When you hear the dial tone, dial “\*98#” followed by the number to which you want to transfer the call.
- 3 After you hear the ring signal or the second party answers it, hang up the phone.

#### 11.14.3.4 USA Three-Way Conference

Use the following steps to make three-way conference calls.

- 1 When you are on the phone talking to someone (party A), press the flash key to put the caller on hold and get a dial tone.
- 2 Dial a phone number directly to make another call (to party B). If you want to have the call use a certain interface (SIP, PSTN or ISDN), enter the SIP, PSTN or ISDN prefix number first.
- 3 When party B answers the second call, press the flash key to create a three-way conversation.
- 4 Hang up the phone to drop the connection.
- 5 If you want to separate the activated three-way conference into two individual connections (with party A on-line and party B on hold), press the flash key.
- 6 If you want to go back to the three-way conversation, press the flash key again.

- 7 If you want to separate the activated three-way conference into two individual connections again, press the flash key. This time the party B is on-line and party A is on hold.

## 11.15 Phone Region Screen

Use this screen to maintain settings that depend on which region of the world the ZyXEL Device is in. To access this screen, click **VoIP > Phone > Region**.

**Figure 111** VoIP > Phone > Region



Each field is described in the following table.

**Table 72** VoIP > Phone > Region

LABEL	DESCRIPTION
Region Settings	Select the place in which the ZyXEL Device is located.
Call Service Mode	Select the mode for supplementary phone services (call hold, call waiting, call transfer and three-way conference calls) that your VoIP service provider supports. <b>Europe Type</b> - use supplementary phone services in European mode <b>USA Type</b> - use supplementary phone services American mode You might have to subscribe to these services to use them. Contact your VoIP service provider.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

## 11.16 Speed Dial

Speed dial provides shortcuts for dialing frequently used (VoIP) phone numbers. You also have to create speed-dial entries if you want to make peer-to-peer calls or call SIP numbers that contain letters. Once you have configured a speed dial rule, you can use a shortcut (the speed dial number, #01 for example) on your phone's keypad to call the phone number. Use this screen to add, edit, or remove speed-dial numbers for outgoing calls. To access this screen, click **VoIP > Phone Book > Speed Dial**.

In peer-to-peer calls, you call another VoIP device directly without going through a VoIP Service provider's SIP server. Select **Non-Proxy (Use IP or URL)** in the **Type** column and enter the callee's IP address or domain name. The ZyXEL Device sends SIP INVITE requests to the peer VoIP device when you use the speed dial entry.

**Figure 112** Phone Book > Speed Dial

Each field is described in the following table.

**Table 73** Phone Book > Speed Dial

LABEL	DESCRIPTION
Speed Dial	Use this section to create or edit speed-dial entries.
#	Select the speed-dial number you want to use for this phone number.
Number	Enter the SIP number you want the ZyXEL Device to call when you dial the speed-dial number.
Name	Enter a name to identify the party you call when you dial the speed-dial number. You can use up to 127 printable ASCII characters.
Type	Select <b>Use Proxy</b> if you want to use one of your SIP accounts to call this phone number. Select <b>Non-Proxy (Use IP or URL)</b> if you want to use a different SIP server or if you want to make a peer-to-peer call. In this case, enter the IP address or domain name of the SIP server or the other party in the field below.
Add	Click this to use the information in the <b>Speed Dial</b> section to update the <b>Speed Dial Phone Book</b> section.
Speed Dial Phone Book	Use this section to look at all the speed-dial entries and to erase them.
Speed Dial	This field displays the speed-dial number you should dial to use this entry.
Number	This field displays the SIP number the ZyXEL Device calls when you dial the speed-dial number.

**Table 73** Phone Book > Speed Dial

LABEL	DESCRIPTION
Name	This field displays the name of the party you call when you dial the speed-dial number.
Destination	This field is blank, if the speed-dial entry uses one of your SIP accounts. Otherwise, this field shows the IP address or domain name of the SIP server or other party. (This field corresponds with the <b>Type</b> field in the <b>Speed Dial</b> section.)
Modify	Use this field to edit or erase the speed-dial entry. Click the <b>Edit</b> icon to copy the information for this speed-dial entry into the <b>Speed Dial</b> section, where you can change it. Click the <b>Remove</b> icon to erase this speed-dial entry.
Clear	Click this to erase all the speed-dial entries.
Cancel	Click this to set every field in this screen to its last-saved value.

## 11.17 Incoming Call Policy Screen

Use this screen to maintain rules for handling incoming calls. You can block, redirect, or accept them. To access this screen, click **VoIP > Phone Book > Incoming Call Policy**.

**Figure 113** Phone Book > Incoming Call Policy

The screenshot shows the 'Incoming Call Policy' tab selected in the top navigation bar. Below the tabs are fields for 'Table Number' (set to 'Table 1') and 'Forward to Number Setup'. This section includes checkboxes for 'Unconditional Forward to Number', 'Busy Forward to Number', and 'No Answer Forward to Number', along with a 'No Answer Waiting Time' input field set to '5 (Second)'. The 'Advanced Setup' section contains a table with 10 rows, each with columns for '#', 'Activate' (checkbox), 'Incoming Call Number' (input field), 'Forward to Number' (input field), and 'Condition' (dropdown menu set to 'Unconditional'). At the bottom are 'Apply' and 'Cancel' buttons.

#	Activate	Incoming Call Number	Forward to Number	Condition
1	<input type="checkbox"/>			Unconditional
2	<input type="checkbox"/>			Unconditional
3	<input type="checkbox"/>			Unconditional
4	<input type="checkbox"/>			Unconditional
5	<input type="checkbox"/>			Unconditional
6	<input type="checkbox"/>			Unconditional
7	<input type="checkbox"/>			Unconditional
8	<input type="checkbox"/>			Unconditional
9	<input type="checkbox"/>			Unconditional
10	<input type="checkbox"/>			Unconditional

You can create two sets of call-forwarding rules. Each one is stored in a call-forwarding table. Each field is described in the following table.

**Table 74** Phone Book > Incoming Call Policy

LABEL	DESCRIPTION
Table Number	Select the call-forwarding table you want to see in this screen. If you change this field, the screen automatically refreshes.
Forward to Number Setup	The ZyXEL Device checks these rules, in the order in which they appear, after it checks the rules in the <b>Advanced Setup</b> section.
Unconditional Forward to Number	Select this if you want the ZyXEL Device to forward all incoming calls to the specified phone number, regardless of other rules in the <b>Forward to Number</b> section. Specify the phone number in the field on the right.
Busy Forward to Number	Select this if you want the ZyXEL Device to forward incoming calls to the specified phone number if the phone port is busy. Specify the phone number in the field on the right. If you have call waiting, the incoming call is forwarded to the specified phone number if you reject or ignore the second incoming call.
No Answer Forward to Number	Select this if you want the ZyXEL Device to forward incoming calls to the specified phone number if the call is unanswered. (See <b>No Answer Waiting Time</b> .) Specify the phone number in the field on the right.
No Answer Waiting Time	This field is used by the <b>No Answer Forward to Number</b> feature and <b>No Answer</b> conditions below. Enter the number of seconds the ZyXEL Device should wait for you to answer an incoming call before it considers the call is unanswered.
Advanced Setup	The ZyXEL Device checks these rules before it checks the rules in the <b>Forward to Number</b> section.
#	This field is a sequential value, and it is not associated with a specific rule. The sequence is important, however. The ZyXEL Device checks each rule in order, and it only follows the first one that applies.
Activate	Select this to enable this rule. Clear this to disable this rule.
Incoming Call Number	Enter the phone number to which this rule applies.
Forward to Number	Enter the phone number to which you want to forward incoming calls from the <b>Incoming Call Number</b> . You may leave this field blank, depending on the <b>Condition</b> .
Condition	Select the situations in which you want to forward incoming calls from the <b>Incoming Call Number</b> , or select an alternative action. <b>Unconditional</b> - The ZyXEL Device immediately forwards any calls from the <b>Incoming Call Number</b> to the <b>Forward to Number</b> . <b>Busy</b> - The ZyXEL Device forwards any calls from the <b>Incoming Call Number</b> to the <b>Forward to Number</b> when your SIP account already has a call connected. <b>No Answer</b> - The ZyXEL Device forwards any calls from the <b>Incoming Call Number</b> to the <b>Forward to Number</b> when the call is unanswered. (See <b>No Answer Waiting Time</b> .) <b>Block</b> - The ZyXEL Device rejects calls from the <b>Incoming Call Number</b> . <b>Accept</b> - The ZyXEL Device allows calls from the <b>Incoming Call Number</b> . You might create a rule with this condition if you do not want incoming calls from someone to be forwarded by rules in the <b>Forward to Number</b> section.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

## 11.18 Distinctive Ring Screen

This screen lets you specify ring types for calls from particular numbers. The ring types vary by ring duration and stop ring duration (the time gap between the rings). Any standard phone is compatible with this feature.

When an incoming call comes in, the ZyXEL Device checks whether it is from any of the phone numbers you set up in this screen. If the number matches an enabled entry, the ZyXEL Device sends the corresponding ring to your phone. You can also configure different rings for calls coming into various SIP accounts, coming into the PSTN line and internal calls.

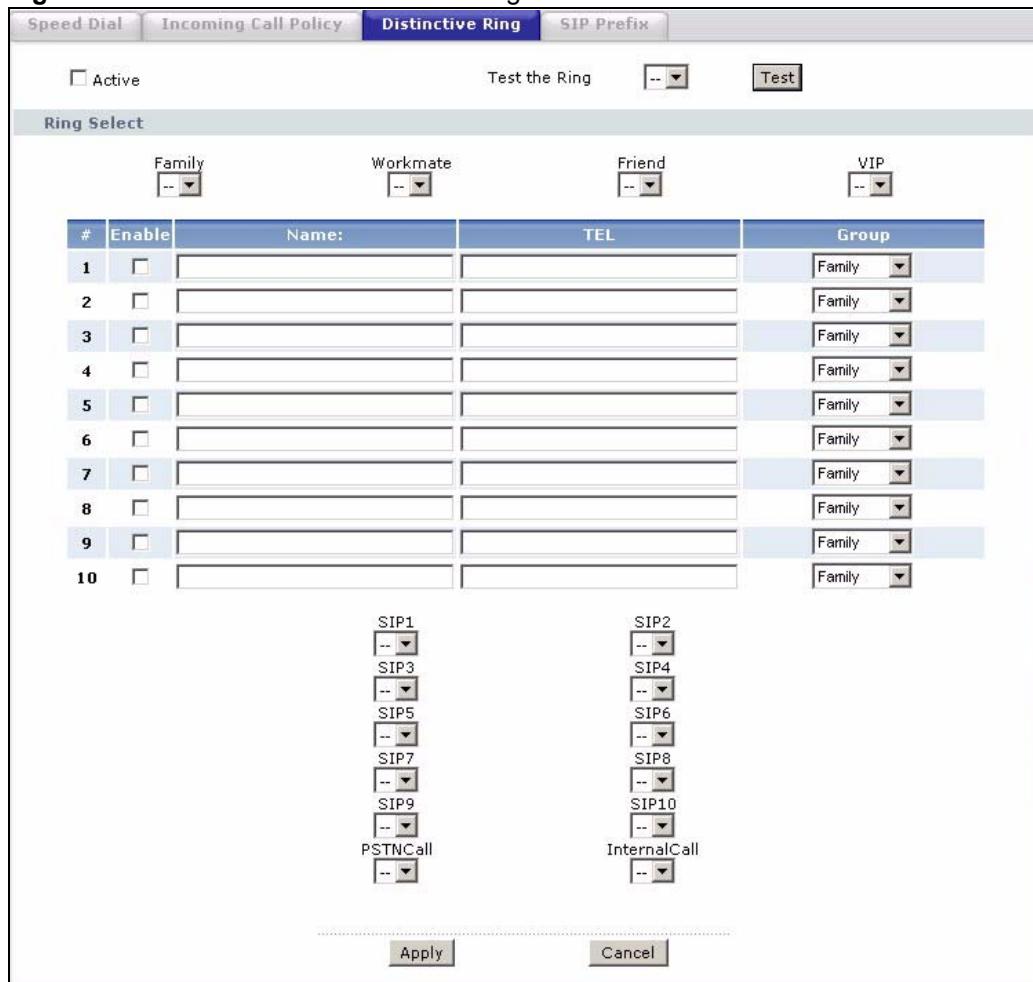


---

The configuration in the Distinctive Ring screen only applies to analog phones connected to the ZyXEL Device.

---

To access this screen, click **VoIP > Phone Book > Distinctive Ring**.

**Figure 114** Phone Book > Distinctive Ring

Each field is described in the following table.

**Table 75** Phone Book > Distinctive Ring

LABEL	DESCRIPTION
Active	Select this if you want to activate the distinctive ring feature. You also have to enable individual entries.
Test the Ring	Use the drop down list box to select the ring tone you would like to hear.
Test	Click this to listen to the ring. All the phones connected to the ZyXEL Device ring when you click this button.
Ring Select	Use this section to first assign rings to groups and then assign phone numbers to those groups.
Family	Select the ring for callers in your family group.
Workmate	Select the ring for callers in your workmate group.
Friend	Select the ring for callers in your friend group.
VIP	Select the ring for callers in your VIP group.
#	This is a read only index number for the phone numbers you assign to different groups.
Enable	Select this to enable your selected distinctive ring for this phone number.

**Table 75** Phone Book > Distinctive Ring

LABEL	DESCRIPTION
Name	Type a name for the associated telephone number.
TEL	Type the telephone number you want to add to a group.
Group	Select a group for the telephone number you entered. You can select <b>Family</b> , <b>Workmate</b> , <b>Friend</b> or <b>VIP</b> .
	You can also select distinctive rings based on whether a call comes from the registered SIP accounts, the PSTN line, or another phone connected to the ZyXEL Device (internal).  <b>Note:</b> The ZyXEL Device will check whether the incoming phone number is part of any of the groups assigned above before checking the incoming line.
SIP1 to SIP 10	Select a ring for each registered SIP account.
PSTN Call	Select a ring for PSTN calls.
Internal Call	Select a ring for internal calls.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 11.19 SIP Prefix Screen

The SIP prefix screen allows you to set up numbers you dial on your phone to specify which SIP account you want to use for a call. If you dial only the phone number (no prefix number) the ZyXEL Device uses default SIP settings to make the call.

Click **VoIP > Phone Book > SIP Prefix**. The following screen displays.

**Figure 115** Phone Book > SIP Prefix

#	Prefix	SIP Index	SIP Domain	Modify
#01		SIP1	profile2.zyxel.com.tw	
#02				
#03				
#04				
#05				
#06				
#07				
#08				
#09				
#10				

Each field is described in the following table.

**Table 76** Phone Book > SIP Prefix

LABEL	DESCRIPTION
SIP Selection by Prefix	
#	Select the index number of the rule you want to edit..
Prefix	Enter the prefix number (1 ~ 8 digits). This is the number you dial before you dial the phone number.
SIP Index	Select the SIP account you want to use to make outgoing calls when you dial the number in the <b>Prefix</b> field.
SIP Domain	This field displays the SIP service domain name you entered when configuring this SIP account.
Add	Click this to use the information in the <b>SIP Selection by Prefix</b> section to update the <b>SIP Prefix Phone Book</b> section.
SIP Prefix Phone Book	This section displays all SIP prefix numbers currently configured on the ZyXEL Device.
#	This is a read-only index number.
Prefix	This field displays the SIP prefix number you dial (before you dial the phone number) in order to use the SIP account specified in the <b>SIP Index</b> field.
SIP Index	This field displays the SIP account used to make outgoing calls when you dial the number in the <b>Prefix</b> field.
SIP Domain	This field displays the SIP domain of the corresponding SIP account.
Modify	Use this field to edit or erase the SIP prefix entry. Click the <b>Edit</b> icon to copy the information for this SIP prefix entry into the <b>SIP Prefix</b> section, where you can change it. Click the <b>Remove</b> icon to erase this SIP prefix entry.

**Table 76** Phone Book > SIP Prefix

LABEL	DESCRIPTION
Clear	Click this to erase all the SIP prefix entries.
Cancel	Click this to set every field in this screen to its last-saved value.

## 11.20 PSTN Line

With the PSTN line you can make and receive regular PSTN phone calls. Use a prefix number to make a regular call. When the device does not have power, you can make regular calls without dialing a prefix number.



When the ZyXEL Device does not have power, only the phone connected to the **PHONE 1** port can be used for making calls. Ensure you know which phone this is, so that in case of emergency you can make outgoing calls.

You can also use the **PSTN Line** screen to specify phone numbers that should always use the regular phone service (without having to dial a prefix number). Do this for emergency numbers (like those for contacting police, fire or emergency medical services).

## 11.21 PSTN Line Screen

Use this screen to set up the PSTN line you use to make regular phone calls. To access this screen, click **VoIP > PSTN Line > General**.

**Figure 116** PSTN Line > General

General	
Call through PSTN Line	
PSTN Line Pre-fix Number	<input type="text" value="0000"/>
Relay to PSTN Line	
1.	<input type="text"/>
2.	<input type="text"/>
3.	<input type="text"/>
4.	<input type="text"/>
5.	<input type="text"/>
6.	<input type="text"/>
7.	<input type="text"/>
8.	<input type="text"/>
9.	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Each field is described in the following table.

**Table 77** PSTN Line > General

LABEL	DESCRIPTION
PSTN Line Pre-fix Number	Enter 1 - 7 numbers you dial before you dial the phone number, if you want to make a regular analog phone call while one of your SIP accounts is registered. These numbers tell the ZyXEL Device that you want to make a regular phone call.
Relay to PSTN Line	Enter phone numbers (for regular calls, not VoIP calls) that you want to dial without the prefix number. For example, you should enter emergency numbers. The number (1 - 9) is not a speed-dial number. It is just a sequential value that is not associated with any phone number.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

## 11.22 ISDN Line Screen

Use this screen to set up the ISDN line you use to make regular phone calls. To access this screen, click **VoIP > ISDN Line**.

**Figure 117** ISDN Line > General

Each field is described in the following table.

**Table 78** ISDN Line > General

LABEL	DESCRIPTION
ISDN Line Pre-fix Number	Enter 1 - 7 numbers you dial before you dial the phone number, if you want to make a regular ISDN phone call while one of your SIP accounts is registered. These numbers tell the ZyXEL Device that you want to make a regular phone call.
Relay to ISDN Line	Enter phone numbers (for regular calls, not VoIP calls) that you want to dial without the prefix number. For example, you should enter emergency numbers. The number (1 - 9) is not a speed-dial number. It is just a sequential value that is not associated with any phone number.

**Table 78** ISDN Line > General

LABEL	DESCRIPTION
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

## 11.23 Fixed Line Numbers

Configure the **Fixed Line Numbers** screen to:

- Use your analog phone(s) to make and receive calls over the ISDN line, using Multiple Subscriber Numbers (MSNs). See [Section 11.23.1 on page 208](#). The MSNs you enter here are used in the **VoIP > Phone > Analog Phone** screen, which you must also configure.
- Use your ISDN phone to receive incoming calls over the analog (PSTN) line. See [Section 11.23.2 on page 209](#).

### 11.23.1 Multiple Subscriber Numbers

MSNs allow you to use two or more phone numbers on one ISDN line. This is similar to conventional extension numbers (for example 0123456 ext. 789). However, MSNs are supplied by your ISDN service provider, and are configured directly in your ISDN devices. They do not require you to use any other equipment.

For example, Alice and Bob subscribe to an ISDN service that gives them an ISDN line (with the phone number 123456) and two MSNs (777 and 888). They connect their ISDN phones directly to the ISDN line. Alice configures her ISDN phone to use one MSN (777) and Bob configures his phone to use the other (888). When someone calls 123456777, only Alice's phone rings, and when someone calls 123456888, only Bob's phone rings.



When you use MSNs with ISDN devices connected to the ZyXEL Device's **ISDN PHONE** port you do not need to configure MSNs in the ZyXEL Device. For details on configuring MSNs on your ISDN device, refer to the documentation provided by its manufacturer.

#### 11.23.1.1 MSNs and the ZyXEL Device

The ZyXEL Device enables you to use analog devices connected to the **PHONE 1** and **PHONE 2** ports to make and receive ISDN calls. You can also use MSNs, if you subscribe to an MSN service.

For example, Carol and David subscribe to an ISDN service that gives them an ISDN line (with the phone number 987654) and two MSNs (333 and 222). However, they do not have ISDN phones. They take the following steps to use analog phones with their ISDN line.

- Carol connects her analog phone to the ZyXEL Device's **PHONE 1** port, and David connects his to the **PHONE 2** port. They connect the ISDN line to the **PSTN/ISDN** port.

- They configure their MSN mappings in the ZyXEL Device's **VoIP > Fixed Line Numbers** screen. Carol maps **MSN1** to "333" and David maps **MSN2** to "222".
- They then configure the **VoIP > Phone > Analog Phone** screen so that the **PHONE 1** port uses the ISDN line and **MSN1** to make and receive calls, and the **PHONE 2** port uses the ISDN line and **MSN2** to make and receive calls.

When someone calls 987654333, only Carol's phone rings, and when someone calls 987654222 only David's phone rings.



You must enter a prefix number in your phone's keypad if you want to make outgoing ISDN calls. Use the **VoIP > ISDN Line** screen to configure this prefix number (see [Section 11.22 on page 207](#)).

### 11.23.2 Receiving Analog Calls With Digital Phones

The ZyXEL Device enables you to receive analog (PSTN) calls with a digital (ISDN) phone as follows.

- 1 Connect an ISDN phone to the **ISDN PHONE** port.
- 2 Click **VoIP > Fixed Line Numbers**.
- 3 In the **PSTN** section, enter a number in the **Number** field (15 digits or fewer, no spaces or dashes allowed). This number must be different from any MSNs you configure in this screen. Click **Apply**.
- 4 On your ISDN phone, set the same number that you configured in the **Number** field as the MSN. Refer to the documentation supplied by your phone's manufacturer for details.

Now, when your ZyXEL Device receives an analog (PSTN) call, your ISDN phone rings.

### 11.23.3 Configuring the Fixed Line Numbers Screen

Click **VoIP > Fixed Line Numbers**. The following screen displays.

**Figure 118** VoIP > Fixed Line Numbers Screen

ISDN		
Item	MSN Number	Brief Description
1	<max 30>	
2	<max 30>	
3	<max 30>	
4	<max 30>	
5	<max 30>	
6	<max 30>	
7	<max 30>	
8	<max 30>	
9	<max 30>	
10	<max 30>	

.....

**Apply**      **Cancel**

The following table describes the labels in this screen.

**Table 79** VoIP > Fixed Line Numbers Screen

LABEL	DESCRIPTION
PSTN	
Number	Configure this field if you want to allow your ISDN phone (connected to the ZyXEL Device's <b>ISDN PHONE</b> port) to receive PSTN calls. Enter a number (up to 15 digits, no hyphens or spaces allowed) that is different from all of your other MSNs and click <b>Apply</b> . Next, configure the MSN in your ISDN phone to use the same number (see your ISDN phone's documentation for details on how to do this). When the ZyXEL Device receives a PSTN call, your ISDN phone rings.
ISDN	
Item	This is the MSN index number you use in the <b>VoIP &gt; Phone &gt; Analog Phone</b> screen.
MSN Number	Enter each Multiple Subscriber Number in these fields as supplied by your ISDN service provider (up to 32 digits, no hyphens or space allowed).
Brief Description	Enter details of the device you want to use with this MSN (for example "personal phone" or "business phone"). This field is for your reference only.
Apply	Click this button to save your changes.
Cancel	Click this button to set the fields in this screen to their last-saved values.

# VoIP Trunking

Use these screens to configure VoIP trunking on your ZyXEL Device.

## 12.1 VoIP Trunking Overview

VoIP trunking connects an IP network (like the Internet) and the Public Switched Telephone Network (PSTN). PSTN includes the world's circuit-switched telephone network which is composed of fixed and mobile telephones. VoIP trunking allows you to create VoIP links which PSTN (Public Switched Telephone Network) callers can use to:

- Make phone calls via the Internet - Make a PSTN call to the ZyXEL Device and it forwards the call to any SIP based VoIP phone.
- Save on long distance calls - The ZyXEL Device creates a VoIP link which can be used to connect to a PSTN phone in another country, province, region and so on.

Similarly, VoIP callers can:

- Make calls to PSTN subscribers at reduced cost - Connect to the ZyXEL Device via VoIP and the ZyXEL Device forwards the call to a PSTN phone.

Creating a link over the IP network requires two VoIP devices. VoIP trunking scenarios vary depending on how the VoIP devices work together and how they receive or forward PSTN calls. The following sections describe the details of VoIP trunking.

## 12.2 VoIP Trunking and Security

Your ZyXEL Device provides two types of authentication to prevent unauthorized callers from using it for VoIP trunking.

### 12.2.1 Auto Attendant and Authentication

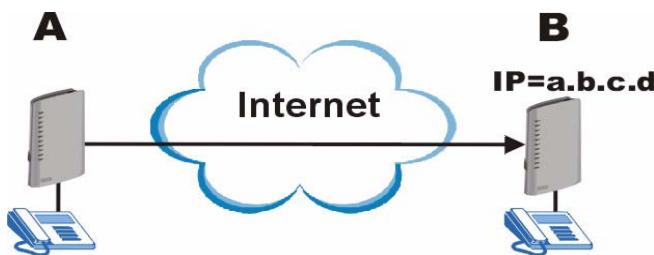
Auto attendant is the ZyXEL Device's name for a service which controls settings specific to VoIP trunking. Most importantly it controls authentication for VoIP trunking. Auto attendant authentication is similar to using a calling card with a PIN (Personal Identification Number). Your ZyXEL Device can be configured so that it prompts callers to enter a PIN (via the phone pad) in order to process any call forwarding requests.

Other settings controlled by the auto attendant include a time limit to decide whether you want to forward a call from the ZyXEL Device or call the phone directly connected to the ZyXEL Device. When you call into your ZyXEL Device you can request to forward a call to another phone number simply by dialing that number. If you don't dial any number within a specified time limit (for example 5 seconds) then the phone directly connected to the ZyXEL Device rings. It also controls the time limit you have between dialing digits of a phone number.

### 12.2.2 Peer Call Authentication

VoIP devices can make peer calls to each other by using the IP address instead of a SIP number to establish a call. The advantage of this is that you do not need to pay a VoIP service provider. VoIP devices that connect using an IP address are referred to here as peer devices. A local peer device is where the VoIP call originates and a remote peer device is where the VoIP call ends. In the following figure, local peer device (A) connects to a remote peer device (B) via the IP address of B.

**Figure 119** Peer Devices Connecting



A peer-to-peer call doesn't require any authentication, however, authentication is required when you request the remote peer device to forward a call. The remote peer device has a list of accounts, each consisting of a username and password, which are allowed to use the remote peer device to forward calls. These accounts make up an incoming authentication list.

The local peer device has a corresponding list of outgoing authentication accounts. These accounts consist of the IP address of a remote peer device, the port number to communicate over as well as a username and password to use for authentication. An outgoing authentication account must match an incoming authentication account's username and password in order for the remote device to forward calls. The following table shows example entries for incoming and outgoing authentication. The bolded entries must match in order for authentication between two peer devices to occur.

**Table 80** Matching Incoming and Outgoing Authentication

ACCOUNT DETAILS	LOCAL PEER DEVICE	REMOTE PEER DEVICE
Outgoing Authentication		
Username	localDeviceA	localDeviceB
Password	passwordA	passwordB
Incoming Authentication		
Username	userone	localDeviceA
Password	userpassword	passwordA

## 12.3 Call Rules

Call rules automate the forwarding of calls, first to a remote peer device and then to PSTN phones. This is used when you make frequent calls to several PSTN numbers in the same geographic area that start with the same numbers (for example an area code). If there is a remote peer device in that area, you can set up a VoIP link to it and have it forward the calls to PSTN phones. This works by configuring a pattern that the ZyXEL Device can recognize. A pattern is just the initial string of digits shared by the phone numbers. The following table shows the relationship between the phone numbers you want to call, the pattern you want to configure and the rule you want to set up.

**Table 81** Call Rules

FREQUENTLY CALLED PSTN NUMBERS	PATTERN	CALL RULE
1-555-555-4321 1-555-544-5678 1-555-432-8888	1555	Set up a peer call to a remote peer device to forward calls starting with the numbers 1555.
1-111-555-4321 1-111-544-5678 1-111-432-8888	1111	Set up a peer call to a remote peer device to forward calls starting with the numbers 1111.

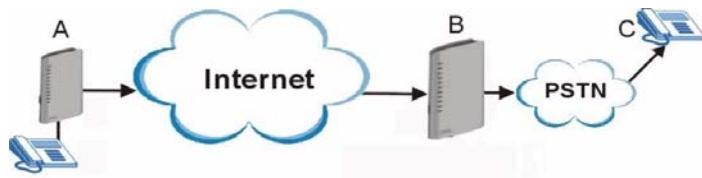
## 12.4 VoIP Trunking Scenarios

There are several different VoIP trunking scenarios.

### 12.4.1 VoIP Phone To PSTN Phone

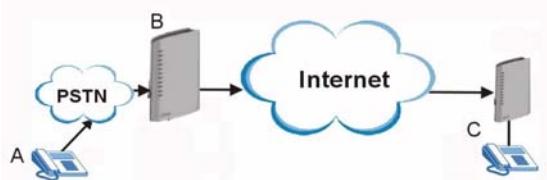
A VoIP phone **A** makes a call to the ZyXEL Device **B** via VoIP. **B** forwards the call to a PSTN phone **C**. **A** can be an analog phone connected to the ZyXEL Device or any other phone capable of making calls over the IP network.

**Figure 120** VoIP Phone To PSTN Phone



### 12.4.2 PSTN Phone To VoIP Phone

A PSTN phone **A** makes a call to the ZyXEL Device **B**. **B** connects **A** to a VoIP phone **C** over the IP network.

**Figure 121** PSTN Phone To VoIP Phone

### 12.4.3 PSTN Phone To PSTN Phone via VoIP

A PSTN phone **A** makes a call to the ZyXEL Device **B**. **B** connects to a peer device **C** and **C** forwards the call to a PSTN phone **D**.

**Figure 122** PSTN Phone To PSTN Phone via VoIP

## 12.5 Trunking General Screen

Use this screen to enable VoIP trunking. Click **VoIP > Trunking > General**.



**VoIP Trunking requires the following additional configuration in the VoIP > SIP > SIP Settings > Advanced Setup screen: Voice Compression field needs to be set to G.729 and DTMF Mode field needs to be set to SIP INFO.**

**Figure 123** VoIP > Trunking > General

General	Peer Call	Call Rule
<b>General</b>		
<input type="checkbox"/> Enable Trunking Auto Attendant Timeout(sec) <input type="text" value="0"/> Dialing Interval(sec) <input type="text" value="0"/> <input type="checkbox"/> Enable Auto Attendant Authentication Password <input type="text"/>	<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Each field is described in the following table.

**Table 82** VoIP > Trunking > General

LABEL	DESCRIPTION
Enable Trunking	Select this to turn on VoIP trunking on your ZyXEL Device.
Auto Attendant Timeout	This is the setting which determines how long the ZyXEL Device waits for a caller to enter a phone number when it receives the call. Enter the number of seconds before the Auto Attendant times out. The default value is 10 seconds and entering 0 does not change the default. Enter a value from 1 to 255 seconds. When the auto attendant times out, the phone directly connected to the ZyXEL Device rings.
Dialing Interval(sec)	Enter the number of seconds the ZyXEL Device should wait after you stop dialing numbers before it makes the phone call. The value depends on how quickly you dial phone numbers. The default value is 3 seconds and entering 0 does not change the default. Enter a value from 1 to 255 seconds.
Enable Auto Attendant Authentication	Select this to enable authentication for calls coming into your ZyXEL Device. This is similar to enabling a PIN (Personal Identification Number) that callers must enter to forward calls via your ZyXEL Device.
Password	This is the PIN callers have to enter via their phone pad when dialing into your ZyXEL Device to forward calls through it. Enter a number between 1 and 32 digits long.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to reset the fields.

## 12.6 Trunking Peer Call Screen

Use this screen to set up outgoing authentication accounts for forwarding calls through peer devices and incoming authentication accounts for forwarding calls from peer devices. To access this screen, click **VoIP > Trunking > Peer Call**.

**Figure 124** VoIP > Trunking > Peer Call

Outgoing Authentication					
#	Name	Username	Password	Peer IP	Peer Port
1				0.0.0.0	5060
2				0.0.0.0	5060
3				0.0.0.0	5060
4				0.0.0.0	5060
5				0.0.0.0	5060
6				0.0.0.0	5060
7				0.0.0.0	5060
8				0.0.0.0	5060
9				0.0.0.0	5060
10				0.0.0.0	5060

Incoming Authentication		
#	Username	Password
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

**Apply**      **Cancel**

Each field is described in the following table.

**Table 83** VoIP > Trunking > Peer Call

LABEL	DESCRIPTION
Outgoing Authentication	You need to set up accounts for the peer devices you use in VoIP trunking. This is the IP address of the remote peer device, as well as the username and password needed to authenticate with the remote peer device.
#	This is an index number of your outgoing authentication accounts.
Name	Enter a descriptive name for the remote peer device of this account. For example, if the peer device is located in London, you might enter <b>London</b> as the account name. This name is used when you configure call rules in the <b>VoIP &gt; Trunking &gt; Call Rules</b> screen.
Username	Enter the username needed to authenticate at the remote peer device. The remote peer device must have the same username in an incoming authentication entry in order to authenticate your connection. Enter up to 32 alphanumeric characters.

**Table 83** VoIP > Trunking > Peer Call (continued)

LABEL	DESCRIPTION
Password	Enter the corresponding password for the username you entered. The remote peer device must have the same password in an incoming authentication entry in order to authenticate your connection. Enter up to 32 alphanumeric characters.
Peer IP	Enter the IP address of the remote peer device which you want to connect to.
Peer Port	Enter the port number through which your ZyXEL Device will connect to the remote peer device. The default value is the standard port for VoIP communication. Do not change this value unless the remote peer device does not follow the standard.
Incoming Authentication	You can set up multiple accounts which are allowed to use your ZyXEL Device for VoIP trunking. When peer devices want to forward calls through your ZyXEL Device, this is the list your ZyXEL Device checks to see if the user has the right to complete the call.
#	This is the index number of the incoming authentication accounts.
Username	Enter a username for the account. This username is used to authenticate peer devices forwarding calls through the ZyXEL Device. Enter up to 32 alphanumeric characters.
Password	Enter the password for the corresponding username. This password is used to authenticate peer devices calling the ZyXEL Device. Enter up to 32 alphanumeric characters.
Apply	Click this to apply your settings to the ZyXEL Device.
Cancel	Click this to reset the fields to their last saved values.

## 12.7 Trunking Call Rule Screen

Use this screen to set up rules that determine which peer VoIP device your call will be forwarded to. To access this screen, click **VoIP > Trunking > Call Rule**.

**Figure 125** VoIP > Trunking > Call Rule

#	Pattern	Account
1		None
2		None
3		None
4		None
5		None
6		None
7		None
8		None
9		None
10		None
11		None
12		None
13		None
14		None
15		None
16		None
17		None
18		None
19		None
20		None

**Apply**      **Cancel**

Each field is described in the following table.

**Table 84** VoIP > Trunking > Call Rule

LABEL	DESCRIPTION
#	This is a read-only index number of the call rules.
Pattern	<p>A <b>Pattern</b> is used when you call your ZyXEL Device from a PSTN phone and want to use it to create a VoIP link to a remote peer device which will forward the call to a PSTN phone.</p> <p>A <b>Pattern</b> is a string of digits your ZyXEL Device uses to determine whether or not to send the call to a peer VoIP device. For example, if you want to use trunking to call phone numbers which start with the number "555", then enter 555 in this field. Enter up to 32 numeric characters.</p> <p>If the number you dial does not match any of the patterns you configured, then you can still use your ZyXEL Device to forward calls to VoIP phones. Simply dial the SIP number of the VoIP phone you want to call.</p>
Account	Select the outgoing authentication account you set up in the <b>Peer Call</b> screen. This account is used to direct your call to the correct remote peer device and to authenticate you. Select <b>None</b> to disable this forwarding rule.
Apply	Click this to apply your settings to the ZyXEL Device.
Cancel	Click this to reset the fields.

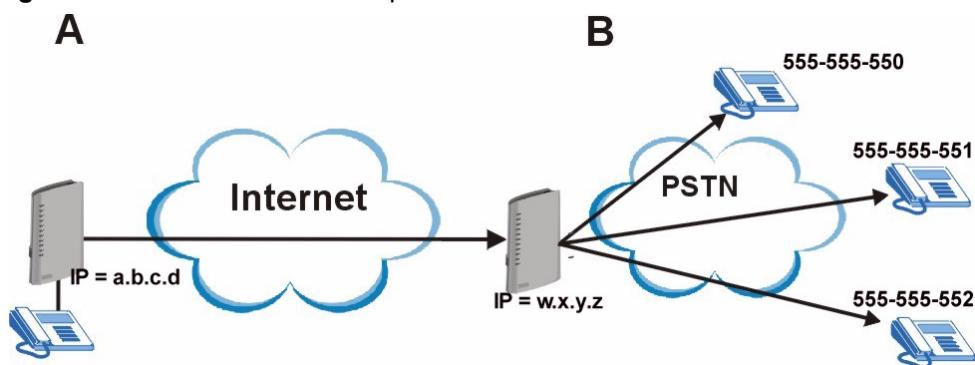
## 12.8 VoIP Trunking Example: VoIP to PSTN

This example shows how to configure VoIP to PSTN trunking to save on long distance calls.

### 12.8.1 Background Information

A company has its headquarters in city A and a branch office in city B. The headquarters often needs to call salespeople employed at the branch office. The sales employees often work away from the office and have PSTN phones (mobile or land based). The two offices have VoIP trunking devices and want to use VoIP trunking to save on calls from the headquarters to their sales team. The head office has a public IP address **a.b.c.d** and the branch office has a public IP address **w.x.y.z**.

**Figure 126** VoIP to PSTN Example



The proposed solution is to establish a peer-to-peer call between the two ZyXEL Devices and have the branch office ZyXEL Device forward calls to the sales team members via PSTN.

### 12.8.2 Configuration Details: Outgoing

The ZyXEL Device (at headquarters) from which the call originates needs to have the following configuration settings:

- 1 Speed dial entries need to be set up for the numbers headquarters wants to call. The destination field of these entries is the IP address of the branch office ZyXEL Device. This must be a non-proxy IP address. The numbers are the phone numbers of the sales team members. This can be configured in the **VoIP > Phone Book > Speed Dial** screen.

**Figure 127** VoIP to PSTN Example - Speed Dial Screen

#	Number	Name	Type
#01			<input checked="" type="radio"/> Use Proxy <input type="radio"/> Non-Proxy (Use IP or URL)
<input type="button" value="Add"/>			

#	Number	Name	Destination	Modify
#01	555555550	Sales1	w.x.y.z	
#02	555555551	Sales2	w.x.y.z	
#03	555555552	Sales2	w.x.y.z	
#04				
#05				
#06				
#07				
#08				
#09				
#10				

- 2 An outgoing authentication account needs to be configured. This account consists of the IP address and port number of the branch office ZyXEL Device as well as the username and password for authentication. This username and password must match the incoming authentication account username and password on the branch office ZyXEL Device. The name of this rule is “CityB” referring to the branch office ZyXEL Device. In this example the username is “headquarters” and the password is “password”. This can be configured in the **VoIP > Trunking > Peer Call** screen.

**Figure 128** VoIP to PSTN Example - Outgoing Authentication

#	Name	Username	Password	Peer IP	Peer Port
1	CityB	headquarters	*****	w.x.y.z	5060
2				0.0.0.0	5060
3				0.0.0.0	5060
4				0.0.0.0	5060
5				0.0.0.0	5060
6				0.0.0.0	5060
7				0.0.0.0	5060
8				0.0.0.0	5060
9				0.0.0.0	5060
10				0.0.0.0	5060

### 12.8.3 Configuration Details: Incoming

The branch office ZyXEL Device needs to have an incoming authentication account configured. This consists of a username and password. This account must match the username and password of the outgoing authentication account of the headquarters’ ZyXEL Device. This can be configured in the **VoIP > Trunking > Peer Call** screen.

**Figure 129** VoIP to PSTN Example - Incoming Authentication

#	Name	Username	Password	Peer IP	Peer Port
1			0.0.0	5060	
2			0.0.0	5060	
9			0.0.0	5060	Suc.
10			0.0.0	5060	

#	Username	Password
1	headquarters	*****
2		

## 12.8.4 Call Progression

The advantage of this kind of VoIP trunking is that once all the configuration is completed, the caller just has to dial a speed dial entry from a phone connected to their ZyXEL Device and the peer devices take care of the rest. This is what happens when headquarters wants to call their **Sales1** employee, which is the first entry in the speed dial screen.

**Table 85** VoIP Trunking Call Progression

HEADQUARTERS	BRANCH OFFICE	SALES1
A person at <b>A</b> dials #01 from the phone connected to the ZyXEL Device.		
The ZyXEL Device at <b>A</b> inspects the number and connects to the remote peer device at <b>B</b> .		
	→	
The remote peer device inspects the number and requests authentication in order to forward the call.		
	←	
The ZyXEL Device at <b>A</b> sends outgoing authentication to the remote peer device.		
	→	
The remote peer device confirms that the username and password match an account in its incoming authentication list.		
	←	
	The remote peer device forwards the call to <b>Sales1</b> .	
	→	
<b>Sales1</b> picks up and the call commences.		
	←	

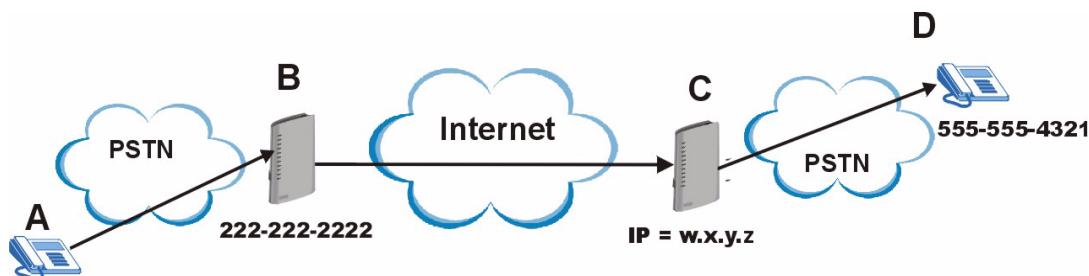
## 12.9 VoIP Trunking Example: PSTN to PSTN via VoIP

This example shows how to configure a PSTN to PSTN call with a VoIP link. It also shows how call rules can be used to automate VoIP trunking.

### 12.9.1 Background Information

A company has its headquarters in one city and a branch office in another. The sales manager (**A**) from headquarters often needs to call salespeople (**D**) employed at the branch office. The sales manager often works away from the headquarters office and the sales employees often work away from the branch office. The sales manager and the sales employees have PSTN phones (mobile or land based). The two offices have VoIP trunking devices. The sales manager wants to use VoIP trunking to save on calls to his sales team. The head office has a ZyXEL Device (**B**) with a PSTN line (tel: 222-222-2222) connected to it. The branch office has a ZyXEL Device (**C**) with a public IP address **w.x.y.z**. The sales employee (**D**) has a PSTN phone with the number 555-555-4321.

**Figure 130** PSTN to PSTN Example



The proposed solution is to configure a call rule which will allow the sales manager to call into the headquarters via PSTN, establish a VoIP link between the two ZyXEL Devices and have the remote peer device forward calls to the sales employee via PSTN.

### 12.9.2 Configuration Details: Outgoing

The ZyXEL Device (at headquarters) from which the VoIP link originates needs to have the following configuration settings:

- 1 Auto attendant authentication needs to be enabled for PSTN calls coming into the headquarters' ZyXEL Device. This ensures that no unauthorized callers use VoIP trunking. In this example the PIN (Personal Identification Number) is set to "12345". The settings dealing with dialing interval and a timeout period are left at default. The ZyXEL Device waits 10 seconds (after initial connection between PSTN caller and the ZyXEL Device) for the PSTN caller to initiate VoIP trunking by dialing another number. It waits 3 seconds between dialing digits before it determines that the entire phone number is entered. These settings can be configured in the **VoIP > Trunking > General** screen.

**Figure 131** PSTN to PSTN Example: General Configuration

<input checked="" type="checkbox"/>	Enable Trunking
	Auto Attendant Timeout(sec) <input type="text" value="10"/>
	Dialing Interval(sec) <input type="text" value="3"/>
<input checked="" type="checkbox"/>	Enable Auto Attendant Authentication
	Password <input type="text" value="12345"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- 2** An outgoing authentication account needs to be configured. This account consists of the IP address and port number of the branch office ZyXEL Device as well as the username and password for authentication. This username and password must match the incoming authentication account username and password on the branch office ZyXEL Device. The name of this account is “CityB” referring to the branch office ZyXEL Device. In this example the username is “headquarters” and the password is “password”. This can be configured in the **VoIP > Trunking > Peer Call** screen.

**Figure 132** PSTN to PSTN Example - Outgoing Authentication

#	Name	Username	Password	Peer IP	Peer Port
1	CityB	headquarters	*****	w.x.y.z	5060
2				0.0.0	5060
3				0.0.0	5060
4				0.0.0	5060
5				0.0.0	5060
6				0.0.0	5060
7				0.0.0	5060
8				0.0.0	5060
9				0.0.0	5060
10				0.0.0	5060

- 3** A call rule needs to be created. This rule tells the ZyXEL Device which remote peer device it should connect to in order to complete the call. This rule is composed of a pattern and an account name. This pattern is simply the first several digits of the number you want the remote device to connect to. In this example this is the first 4 digits (“5555”) of “Sales1” telephone number. The account name is the name of the outgoing authentication account created in the **Speed Dial** screen (“CityB”). This setting can be configured in the **VoIP > Trunking > Call Rule** screen.

**Figure 133** PSTN to PSTN Example - Call Rule

#	Pattern	Account
1	5555	CityB
2		None
3		None
4		None
5		None
6		None
7		None
8		None
9		None

### 12.9.3 Configuration Details: Incoming

The branch office ZyXEL Device needs to have an incoming authentication account configured. This consists of a username and password. This account must match the username and password of the outgoing authentication account of the headquarters' ZyXEL Device. This can be configured in the **VoIP > Trunking > Peer Call** screen.

**Figure 134** PSTN to PSTN Example - Incoming Authentication

#	Name	Username	Password	Peer IP	Peer Port
1				0.0.0.0	5060
2				0.0.0.0	5060
9				0.0.0.0	5060
10				0.0.0.0	5060

#	Username	Password
1	headquarters	*****
2		

### 12.9.4 Call Progression

The call is initiated by the manager dialing into the headquarter's ZyXEL Device via PSTN. In this scenario a VoIP link is established between headquarters and the branch office and then the call is forwarded to **Sales1** using PSTN.

**Table 86** PSTN to PSTN: VoIP Trunking Call Progression

MANAGER	HEADQUARTERS	BRANCH OFFICE	SALES1
	The manager dials the PSTN number of the headquarters' ZyXEL Device. <b>(222-222-2222)</b>		
	The ZyXEL Device receives the call and sends a ringback alert tone to indicate to the caller that VoIP trunking is enabled.		
	The manager dials the PSTN number of <b>Sales1 (555-555-1234)</b> .		
	The ZyXEL Device prompts the manager to enter the PIN in order to allow VoIP trunking.		
	The manager dials the PIN <b>(12345)</b> .		
	The ZyXEL Device confirms the password and allows for VoIP trunking. The ZyXEL Device inspects the phone number against call rules. Since the number starts with the pattern <b>(5555)</b> , it uses the account <b>(CityB)</b> associated with this pattern to connect the call to the remote peer device at the branch office.		
	The remote peer device inspects the number and requests authentication in order to forward the call.		
	The ZyXEL Device at <b>A</b> sends outgoing authentication to the remote peer device.		
	The remote peer device confirms that the username and password match an account in its incoming authentication list.		
		The remote peer device forwards the call to <b>Sales1</b> .	
<b>Sales1</b> picks up and the call commences.			



# Phone Usage

This chapter describes how to use a phone connected to your ZyXEL Device for basic tasks.

## 13.1 Dialing a Telephone Number

The **PHONE** LED turns green when your SIP account is registered. Dial a SIP number like “12345” on your phone’s keypad.

Use speed dial entries (see [Section 11.16 on page 198](#)) for peer-to-peer calls or SIP numbers that use letters. Dial the speed dial entry on your telephone’s keypad.

Use your VoIP service provider’s dialing plan to call regular telephone numbers.

## 13.2 Using Speed Dial to Dial a Telephone Number

After configuring the speed dial entry and adding it to the phonebook, press the speed dial entry’s key combination on your phone’s keypad.

## 13.3 Internal Calls

When you have more than one phone connected to the ZyXEL Device’s phone ports, you can make internal calls from a phone connected to one port to a phone connected to another.



When you have more than one phone connected to a single analog PHONE port, they behave exactly the same as one another. The extension number you give to the port applies to all the phones connected to it. However, when you have multiple ISDN phones connected to the ISDN port, each can have its own extension number. See [Section 11.12 on page 191](#) for more information.

The ZyXEL Device supports the following functions for internal calls:

- Phone Book
- Call Transfer
- Call Forwarding

- Follow Me
- Call Pickup



---

To use these supplementary functions for internal calls, you have to configure the **VoIP > Phone > Ext. Table** first.

---

### 13.3.1 Phone Book

You can assign each phone connected to the ZyXEL Device an extension number and make internal calls between these phones. You can also call a group of phones that share the same group number. For information on how to configure extension numbers and group numbers, refer to [Section 11.12 on page 191](#).



---

If you don't configure the extension table, you can press "#####" on your phone's keypad to call all the phones connecting to the ZyXEL Device's phone ports.

---

### 13.3.2 Call Transfer

Take the following steps to transfer an ongoing call to another extension number.

- 1 Press your phone's flash key to put the caller on hold.
- 2 When you hear the dial tone, dial "\*98#" followed by the number to which you want to transfer the call.
- 3 After you hear the ring signal or the second party answers it, hang up the phone.

### 13.3.3 Call Forwarding

You can set the ZyXEL Device to forward calls to a specific extension number, either unconditionally (always), when your number is busy, or when you do not answer. You can also forward incoming calls from one specified number to another. Configure your call-forwarding rules in the **VoIP > Phone > Ext. Table > Advanced** screen.

### 13.3.4 Follow Me

When you have to leave your seat temporarily, you can set the ZyXEL Device to unconditionally forward calls to another specific extension number. You can set up "follow me" either on your phone, or on the phone to which you want calls forwarded.

- Local setting (when you are at your phone):

When you hear the dial tone, dial "\*01" followed by the number to which you want the call to be forwarded. When you do not need the follow me function, dial "#01" to cancel this rule.

- Remote setting (when you are at another place):  
When you hear the dial tone, dial “\*04” followed by your extension number.  
When you do not need the follow me function, dial “#04” followed by your extension number to cancel this rule.

### 13.3.5 Call Pickup

When an incoming internal call rings but the user of the phone is unavailable to receive the call, you can pick the phone up for this person.

Take the following steps to receive incoming internal calls from your phone.

- 1 If the ringing phone does not belong to the same group of your phone but you know its extension number, press “\*97#” followed by the extension number of the ringing phone to receive the call.
- 2 If the ringing phone belongs to the same group of your phone, press “\*97#” to receive the call.

## 13.4 Checking the Device’s IP Address

Do the following to listen to the ZyXEL Device’s current IP address.

- 1 Pick up your phone’s receiver.
- 2 Press “\*\*\*\*\*” on your phone’s keypad and wait for the message that says you are in the configuration menu.
- 3 Press “5” followed by the # key.
- 4 Listen to the IP address and make a note of it.
- 5 Hang up the receiver.

## 13.5 Auto Firmware Upgrade

During auto-provisioning, the ZyXEL Device checks to see if there is a newer firmware version. If newer firmware is available, the ZyXEL Device plays a recording when you pick up your phone’s handset.

Press “\*99#” to upgrade the ZyXEL Device’s firmware.

Press “#99#” to not upgrade the ZyXEL Device’s firmware.



---

# PART V

# Security

---

- Firewalls (233)
- Firewall Configuration (245)
- Content Filtering (265)
- Introduction to IPSec (269)
- VPN Screens (275)
- Certificates (301)



# Firewalls

This chapter gives some background information on firewalls and introduces the ZyXEL Device firewall.

## 14.1 Firewall Overview

Originally, the term “firewall” referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term “firewall” is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an untrusted network. Of course, firewalls cannot solve every security problem. A firewall is *one* of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the *only* mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

Refer to [Section 15.5 on page 248](#) to configure default firewall settings.

Refer to [Section 15.6 on page 249](#) to view firewall rules.

Refer to [Section 15.6.1 on page 251](#) to configure firewall rules.

Refer to [Section 15.6.2 on page 254](#) to configure a custom service.

Refer to [Section 15.8.3 on page 260](#) to configure firewall thresholds.

## 14.2 Types of Firewalls

There are three main types of firewalls:

- Packet Filtering Firewalls
- Application-level Firewalls
- Stateful Inspection Firewalls

### 14.2.1 Packet Filtering Firewalls

Packet filtering firewalls restrict access based on the source/destination computer network address of a packet and the type of application.

### 14.2.2 Application-level Firewalls

Application-level firewalls restrict access by serving as proxies for external servers. Since they use programs written for specific Internet services, such as HTTP, FTP and telnet, they can evaluate network packets for valid application-specific data. Application-level gateways have a number of general advantages over the default mode of permitting application traffic directly to internal hosts:

Information hiding prevents the names of internal systems from being made known via DNS to outside systems, since the application gateway is the only host whose name must be made known to outside systems.

Robust authentication and logging pre-authenticates application traffic before it reaches internal hosts and causes it to be logged more effectively than if it were logged with standard host logging. Filtering rules at the packet filtering router can be less complex than they would be if the router needed to filter application traffic and direct it to a number of specific systems. The router need only allow application traffic destined for the application gateway and reject the rest.

### 14.2.3 Stateful Inspection Firewalls

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency, however, they may lack the granular application level access control or caching that some proxies support. See [Section 14.5 on page 238](#) for more information on stateful inspection.

Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

## 14.3 Introduction to ZyXEL's Firewall

The ZyXEL Device firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated. The ZyXEL Device's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The ZyXEL Device can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network. The ZyXEL Device also has packet filtering capabilities.

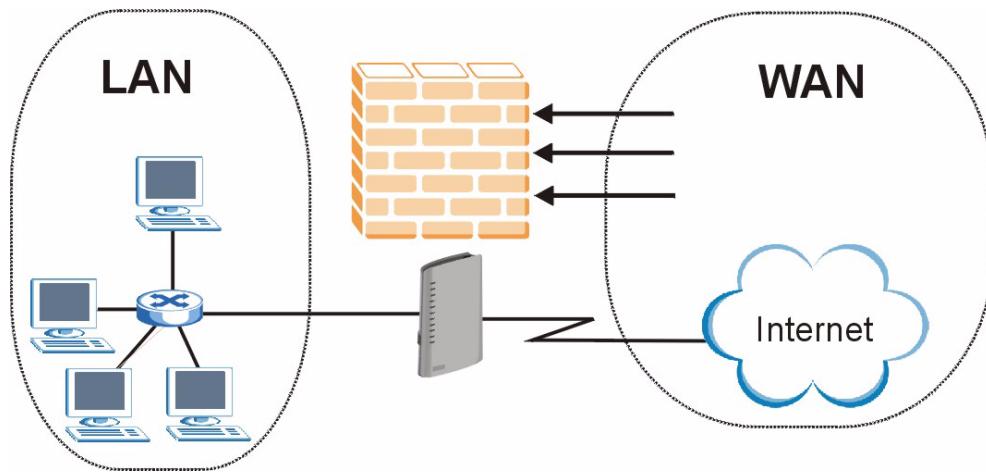
The ZyXEL Device is installed between the LAN and the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The ZyXEL Device has one DSL/ISDN port and one Ethernet LAN port, which physically separate the network into two areas.

- The DSL/ISDN port connects to the Internet.
- The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP, and the World Wide Web. However, "inbound access" will not be allowed unless you configure remote management or create a firewall rule to allow a remote host to use a specific service.

### 14.3.1 Denial of Service Attacks

**Figure 135** Firewall Application



## 14.4 Denial of Service

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The ZyXEL Device is pre-configured to automatically detect and thwart all known DoS attacks.

### 14.4.1 Basics

Computers share information over the Internet using a common language called TCP/IP. TCP/IP, in turn, is a set of application protocols that perform specific functions. An “extension number”, called the "TCP port" or "UDP port" identifies these protocols, such as HTTP (Web), FTP (File Transfer Protocol), POP3 (E-mail), etc. For example, Web traffic by default uses TCP port 80.

When computers communicate on the Internet, they are using the client/server model, where the server "listens" on a specific TCP/UDP port for information requests from remote client computers on the network. For example, a Web server typically listens on port 80. Please note that while a computer may be intended for use over a single port, such as Web on port 80, other ports are also active. If the person configuring or managing the computer is not careful, a hacker could attack it over an unprotected port.

Some of the most common IP ports are:

**Table 87** Common IP Ports

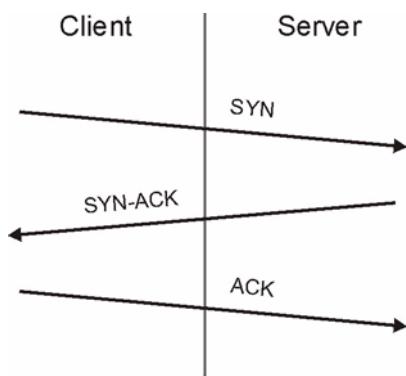
21	FTP	53	DNS
23	Telnet	80	HTTP
25	SMTP	110	POP3

### 14.4.2 Types of DoS Attacks

There are four types of DoS attacks:

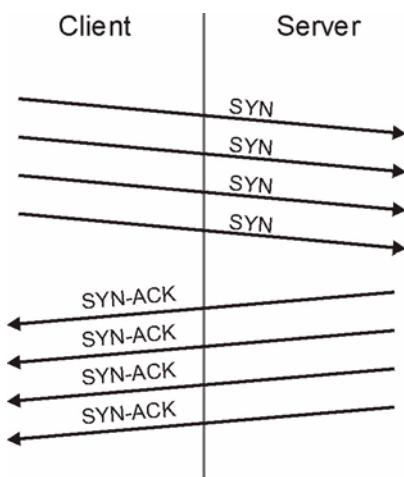
- 1 Those that exploit bugs in a TCP/IP implementation.
- 2 Those that exploit weaknesses in the TCP/IP specification.
- 3 Brute-force attacks that flood a network with useless data.
- 4 IP Spoofing.
- 5 "**Ping of Death**" and "**Teardrop**" attacks exploit bugs in the TCP/IP implementations of various computer and host systems.
  - Ping of Death uses a "ping" utility to create an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. Systems may crash, hang or reboot.
  - Teardrop attack exploits weaknesses in the re-assembly of IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original IP packet except that it contains an offset field that says, for instance, "This fragment is carrying bytes 200 through 400 of the original (non fragmented) IP packet." The Teardrop program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination, some systems will crash, hang, or reboot.
- 6 Weaknesses in the TCP/IP specification leave it open to "**SYN Flood**" and "**LAND**" attacks. These attacks are executed during the handshake that initiates a communication session between two applications.

**Figure 136** Three-Way Handshake

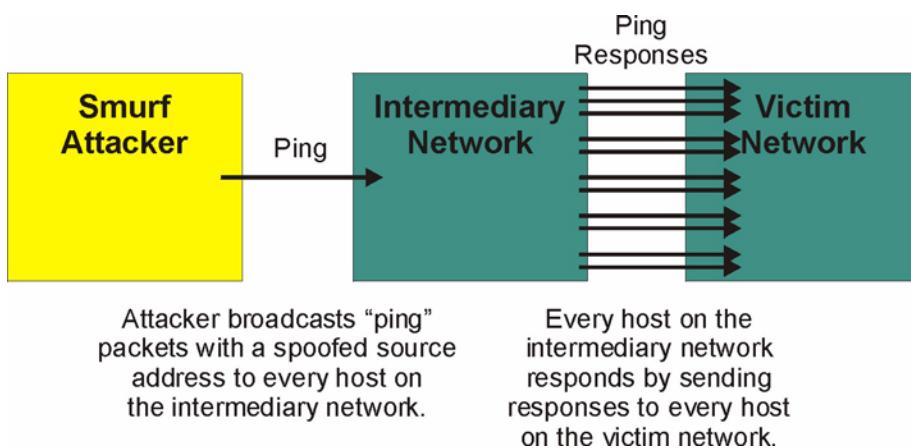


Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

- **SYN Attack** floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set at relatively long intervals) terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

**Figure 137** SYN Flood

- In a **LAND Attack**, hackers flood SYN packets into the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.
- 7 A **brute-force** attack, such as a "Smurf" attack, targets a feature in the IP specification known as directed or subnet broadcasting, to quickly flood the target network with useless data. A Smurf hacker floods a router with Internet Control Message Protocol (ICMP) echo request packets (pings). Since the destination IP address of each packet is the broadcast address of the network, the router will broadcast the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large amount of ICMP echo request and response traffic. If a hacker chooses to spoof the source IP address of the ICMP echo request packet, the resulting ICMP traffic will not only clog up the "intermediary" network, but will also congest the network of the spoofed source IP address, known as the "victim" network. This flood of broadcast traffic consumes all available bandwidth, making communications impossible.

**Figure 138** Smurf Attack

#### 14.4.2.1 ICMP Vulnerability

ICMP is an error-reporting protocol that works in concert with IP. The following ICMP types trigger an alert:

**Table 88** ICMP Commands That Trigger Alerts

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

#### 14.4.2.2 Illegal Commands (NetBIOS and SMTP)

The only legal NetBIOS commands are the following - all others are illegal.

**Table 89** Legal NetBIOS Commands

MESSAGE:
REQUEST:
POSITIVE:
VE:
RETARGET:
KEEPALIVE:

All SMTP commands are illegal except for those displayed in the following tables.

**Table 90** Legal SMTP Commands

AUTH	DATA	EHLO	ETRN	EXPN	HELO	HELP	MAIL	NOOP
QUIT	RCPT	RSET	SAML	SEND	SOML	TURN	VRFY	

#### 14.4.2.3 Traceroute

Traceroute is a utility used to determine the path a packet takes between two endpoints. Sometimes when a packet filter firewall is configured incorrectly an attacker can traceroute the firewall gaining knowledge of the network topology inside the firewall.

Often, many DoS attacks also employ a technique known as "**IP Spoofing**" as part of their attack. IP Spoofing may be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by tricking a router or firewall into thinking that the communications are coming from within the trusted network. To engage in IP spoofing, a hacker must modify the packet headers so that it appears that the packets originate from a trusted host and should be allowed through the router or firewall. The ZyXEL Device blocks all IP Spoofing attempts.

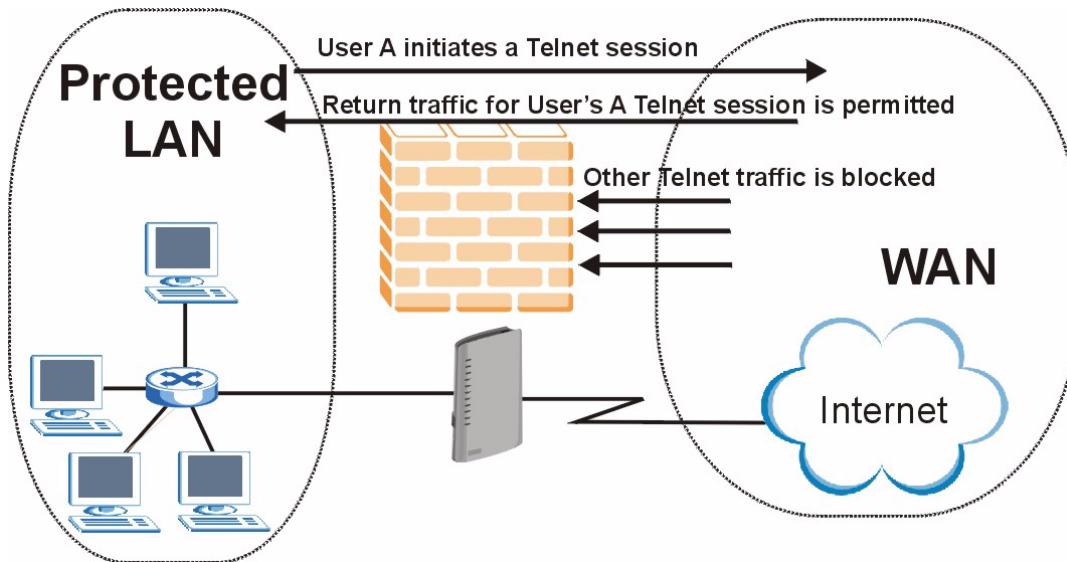
### 14.5 Stateful Inspection

With stateful inspection, fields of the packets are compared to packets that are already known to be trusted. For example, if you access some outside service, the proxy server remembers things about your original request, like the port number and source and destination addresses. This "remembering" is called *saving the state*. When the outside system responds to your request, the firewall compares the received packets with the saved state to determine if they

are allowed in. The ZyXEL Device uses stateful packet inspection to protect the private LAN from hackers and vandals on the Internet. By default, the ZyXEL Device's stateful inspection allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet. In summary, stateful inspection:

- Allows all sessions originating from the LAN (local network) to the WAN (Internet).
- Denies all sessions originating from the WAN to the LAN.

**Figure 139** Stateful Inspection



The previous figure shows the ZyXEL Device's default firewall rules in action as well as demonstrates how stateful inspection works. User A can initiate a Telnet session from within the LAN and responses to this request are allowed. However other Telnet traffic initiated from the WAN is blocked.

#### 14.5.1 Stateful Inspection Process

In this example, the following sequence of events occurs when a TCP packet leaves the LAN network through the firewall's WAN interface. The TCP packet is the first in a session, and the packet's application layer protocol is configured for a firewall rule inspection:

- 1 The packet travels from the firewall's LAN to the WAN.
- 2 The packet is evaluated against the interface's existing outbound access list, and the packet is permitted (a denied packet would simply be dropped at this point).
- 3 The packet is inspected by a firewall rule to determine and record information about the state of the packet's connection. This information is recorded in a new state table entry created for the new connection. If there is not a firewall rule for this packet and it is not an attack, then the settings in the **Firewall General** screen determine the action for this packet.
- 4 Based on the obtained state information, a firewall rule creates a temporary access list entry that is inserted at the beginning of the WAN interface's inbound extended access list. This temporary access list entry is designed to permit inbound packets of the same connection as the outbound packet just inspected.
- 5 The outbound packet is forwarded out through the interface.

- 6 Later, an inbound packet reaches the interface. This packet is part of the connection previously established with the outbound packet. The inbound packet is evaluated against the inbound access list, and is permitted because of the temporary access list entry previously created.
- 7 The packet is inspected by a firewall rule, and the connection's state table entry is updated as necessary. Based on the updated state information, the inbound extended access list temporary entries might be modified, in order to permit only packets that are valid for the current state of the connection.
- 8 Any additional inbound or outbound packets that belong to the connection are inspected to update the state table entry and to modify the temporary inbound access list entries as required, and are forwarded through the interface.
- 9 When the connection terminates or times out, the connection's state table entry is deleted and the connection's temporary inbound access list entries are deleted.

### 14.5.2 Stateful Inspection on Your ZyXEL Device

Additional rules may be defined to extend or override the default rules. For example, a rule may be created which will:

- Block all traffic of a certain type, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic from the Internet to specific hosts on the LAN.
- Allow access to a Web server to everyone but competitors.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by evaluating the network traffic's Source IP address, Destination IP address, IP protocol type, and comparing these to rules set by the administrator.



The ability to define firewall rules is a very powerful tool. Using custom rules, it is possible to disable all firewall protection or block all access to the Internet. Use extreme caution when creating or deleting firewall rules. Test changes after creating them to make sure they work correctly.

Below is a brief technical description of how these connections are tracked. Connections may either be defined by the upper protocols (for instance, TCP), or by the ZyXEL Device itself (as with the "virtual connections" created for UDP and ICMP).

### 14.5.3 TCP Security

The ZyXEL Device uses state information embedded in TCP packets. The first packet of any new connection has its SYN flag set and its ACK flag cleared; these are "initiation" packets. All packets that do not have this flag structure are called "subsequent" packets, since they represent data that occurs later in the TCP stream.

If an initiation packet originates on the WAN, this means that someone is trying to make a connection from the Internet into the LAN. Except in a few special cases (see "Upper Layer Protocols" shown next), these packets are dropped and logged.

If an initiation packet originates on the LAN, this means that someone is trying to make a connection from the LAN to the Internet. Assuming that this is an acceptable part of the security policy (as is the case with the default policy), the connection will be allowed. A cache entry is added which includes connection information such as IP addresses, TCP ports, sequence numbers, etc.

When the ZyXEL Device receives any subsequent packet (from the Internet or from the LAN), its connection information is extracted and checked against the cache. A packet is only allowed to pass through if it corresponds to a valid connection (that is, if it is a response to a connection which originated on the LAN).

#### 14.5.4 UDP/ICMP Security

UDP and ICMP do not themselves contain any connection information (such as sequence numbers). However, at the very minimum, they contain an IP address pair (source and destination). UDP also contains port pairs, and ICMP has type and code information. All of this data can be analyzed in order to build "virtual connections" in the cache.

For instance, any UDP packet that originates on the LAN will create a cache entry. Its IP address and port pairs will be stored. For a short period of time, UDP packets from the WAN that have matching IP and UDP information will be allowed back in through the firewall.

A similar situation exists for ICMP, except that the ZyXEL Device is even more restrictive. Specifically, only outgoing echoes will allow incoming echo replies, outgoing address mask requests will allow incoming address mask replies, and outgoing timestamp requests will allow incoming timestamp replies. No other ICMP packets are allowed in through the firewall, simply because they are too dangerous and contain too little tracking information. For instance, ICMP redirect packets are never allowed in, since they could be used to reroute traffic through attacking machines.

#### 14.5.5 Upper Layer Protocols

Some higher layer protocols (such as FTP and RealAudio) utilize multiple network connections simultaneously. In general terms, they usually have a "control connection" which is used for sending commands between endpoints, and then "data connections" which are used for transmitting bulk information.

Consider the FTP protocol. A user on the LAN opens a control connection to a server on the Internet and requests a file. At this point, the remote server will open a data connection from the Internet. For FTP to work properly, this connection must be allowed to pass through even though a connection from the Internet would normally be rejected.

In order to achieve this, the ZyXEL Device inspects the application-level FTP data. Specifically, it searches for outgoing "PORT" commands, and when it sees these, it adds a cache entry for the anticipated data connection. This can be done safely, since the PORT command contains address and port information, which can be used to uniquely identify the connection.

Any protocol that operates in this way must be supported on a case-by-case basis. You can use the web configurator's Custom Ports feature to do this.

## 14.6 Guidelines for Enhancing Security with Your Firewall

- Change the default password.
- Limit who can telnet into your router.
- Don't enable any local service (such as SNMP or NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
- For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
- Protect against IP spoofing by making sure the firewall is active.
- Keep the firewall in a secured (locked) room.

### 14.6.1 Security In General

You can never be too careful! Factors outside your firewall, filtering or NAT can cause security breaches. Below are some generalizations about what you can do to minimize them.

- Encourage your company or organization to develop a comprehensive security plan. Good network administration takes into account what hackers can do and prepares against attacks. The best defense against hackers and crackers is information. Educate all employees about the importance of security and how to minimize risk. Produce lists like this one!
- DSL or cable modem connections are “always-on” connections and are particularly vulnerable because they provide more opportunities for hackers to crack your system. Turn your computer off when not in use.
- Never give out a password or any sensitive information to an unsolicited telephone call or e-mail.
- Never e-mail sensitive information such as passwords, credit card information, etc., without encrypting the information first.
- Never submit sensitive information via a web page unless the web site uses secure connections. You can identify a secure connection by looking for a small “key” icon on the bottom of your browser (Internet Explorer 3.02 or better or Netscape 3.0 or better). If a web site uses a secure connection, it is safe to submit information. Secure web transactions are quite difficult to crack.
- Never reveal your IP address or other system networking information to people outside your company. Be careful of files e-mailed to you from strangers. One common way of getting BackOrifice on a system is to include it as a Trojan horse with other files.
- Change your passwords regularly. Also, use passwords that are not easy to figure out. The most difficult passwords to crack are those with upper and lower case letters, numbers and a symbol such as % or #.
- Upgrade your software regularly. Many older versions of software, especially web browsers, have well known security deficiencies. When you upgrade to the latest versions, you get the latest patches and fixes.
- If you use “chat rooms” or IRC sessions, be careful with any information you reveal to strangers.
- If your system starts exhibiting odd behavior, contact your ISP. Some hackers will set off hacks that cause your system to slowly become unstable or unusable.

- Always shred confidential information, particularly about your computer, before throwing it away. Some hackers dig through the trash of companies or individuals for information that might help them in an attack.

## 14.7 Packet Filtering Vs Firewall

Below are some comparisons between the ZyXEL Device's filtering and firewall functions.

### 14.7.1 Packet Filtering:

- The router filters packets as they pass through the router's interface according to the filter rules you designed.
- Packet filtering is a powerful tool, yet can be complex to configure and maintain, especially if you need a chain of rules to filter a service.
- Packet filtering only checks the header portion of an IP packet.

#### 14.7.1.1 When To Use Filtering

- To block/allow LAN packets by their MAC addresses.
- To block/allow special IP packets which are neither TCP nor UDP, nor ICMP packets.
- To block/allow both inbound (WAN to LAN) and outbound (LAN to WAN) traffic between the specific inside host/network "A" and outside host/network "B". If the filter blocks the traffic from A to B, it also blocks the traffic from B to A. Filters can not distinguish traffic originating from an inside host or an outside host by IP address.
- To block/allow IP trace route.

### 14.7.2 Firewall

- The firewall inspects packet contents as well as their source and destination addresses. Firewalls of this type employ an inspection module, applicable to all protocols, that understands data in the packet intended for other layers, from the network layer (IP headers) up to the application layer.
- The firewall performs stateful inspection. It takes into account the state of connections it handles so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and allowed in. Conversely, an incoming packet masquerading as a response to a nonexistent outbound request can be blocked.
- The firewall uses session filtering; smart rules that enhance the filtering process and control the network session rather than control individual packets in a session.
- The firewall provides e-mail service to notify you of routine reports and when alerts occur.

#### 14.7.2.1 When To Use The Firewall

- To prevent DoS attacks and prevent hackers cracking your network.
- A range of source and destination IP addresses as well as port numbers can be specified within one firewall rule making the firewall a better choice when complex rules are required.

- To selectively block/allow inbound or outbound traffic between inside host/networks and outside host/networks. Remember that filters can not distinguish traffic originating from an inside host or an outside host by IP address.
- The firewall performs better than filtering if you need to check many rules.
- Use the firewall if you need routine e-mail reports about your system or need to be alerted when attacks occur.
- The firewall can block specific URL traffic that might occur in the future. The URL can be saved in an Access Control List (ACL) database.

# Firewall Configuration

This chapter shows you how to enable and configure the ZyXEL Device firewall.

## 15.1 Access Methods

The web configurator is, by far, the most comprehensive firewall configuration tool your ZyXEL Device has to offer. For this reason, it is recommended that you configure your firewall using the web configurator. CLI commands provide limited configuration options and are only recommended for advanced users.

## 15.2 General Firewall Policy Overview

Firewall rules are grouped based on the direction of travel of packets to which they apply:

- LAN to LAN/ Router
- WAN to LAN
- LAN to WAN
- WAN to WAN/ Router



---

The LAN includes both the LAN port and the WLAN.

---

By default, the ZyXEL Device's stateful packet inspection allows packets traveling in the following directions:

- LAN to LAN/ Router

This allows computers on the LAN to manage the ZyXEL Device and communicate between networks or subnets connected to the LAN interface.

- LAN to WAN

By default, the ZyXEL Device's stateful packet inspection drops packets traveling in the following directions:

- WAN to LAN
- WAN to WAN/ Router

This prevents computers on the WAN from using the ZyXEL Device as a gateway to communicate with other computers on the WAN and/or managing the ZyXEL Device.

You may define additional rules and sets or modify existing ones but please exercise extreme caution in doing so.



---

If you configure firewall rules without a good understanding of how they work, you might inadvertently introduce security risks to the firewall and to the protected network. Make sure you test your rules after you configure them.

---

For example, you may create rules to:

- Block certain types of traffic, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
- Allow everyone except your competitors to access a Web server.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by comparing the Source IP address, Destination IP address and IP protocol type of network traffic to rules set by the administrator. Your customized rules take precedence and override the ZyXEL Device's default rules.

## 15.3 Rule Logic Overview



---

Study these points carefully before configuring rules.

---

### 15.3.1 Rule Checklist

State the intent of the rule. For example, "This restricts all IRC access from the LAN to the Internet." Or, "This allows a remote Lotus Notes server to synchronize over the Internet to an inside Notes server."

- 1 Is the intent of the rule to forward or block traffic?
- 2 What direction of traffic does the rule apply to?
- 3 What IP services will be affected?
- 4 What computers on the LAN are to be affected (if any)?
- 5 What computers on the Internet will be affected? The more specific, the better. For example, if traffic is being allowed from the Internet to the LAN, it is better to allow only certain machines on the Internet to access the LAN.

### 15.3.2 Security Ramifications

- 1 Once the logic of the rule has been defined, it is critical to consider the security ramifications created by the rule:

- 2** Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
- 3** Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
- 4** Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
- 5** Does this rule conflict with any existing rules?
- 6** Once these questions have been answered, adding rules is simply a matter of plugging the information into the correct fields in the web configurator screens.

### 15.3.3 Key Fields For Configuring Rules

#### 15.3.3.1 Action

Should the action be to **Drop**, **Reject** or **Permit**?



“Drop” means the firewall silently discards the packet. “Reject” means the firewall discards packets and sends an ICMP destination-unreachable message to the sender.

#### 15.3.3.2 Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it. See [Appendix E on page 475](#) for more information on predefined services.

#### 15.3.3.3 Source Address

What is the connection’s source address; is it on the LAN or WAN? Is it a single IP, a range of IPs or a subnet?

#### 15.3.3.4 Destination Address

What is the connection’s destination address; is it on the LAN or WAN? Is it a single IP, a range of IPs or a subnet?

## 15.4 Connection Direction

This section describes examples for firewall rules for connections going from LAN to WAN and from WAN to LAN.

LAN to LAN/ Router, WAN to WAN/ Router and DMZ to DMZ/ Router rules apply to packets coming in on the associated interface (LAN, WAN or DMZ respectively). LAN to LAN/ Router means policies for LAN-to-ZyXEL Device (the policies for managing the ZyXEL Device through the LAN interface) and policies for LAN-to-LAN (the policies that control routing between two subnets on the LAN). Similarly, WAN to WAN/ Router and DMZ to DMZ/ Router policies apply in the same way to the WAN and DMZ ports.

### 15.4.1 LAN to WAN Rules

The default rule for LAN to WAN traffic is that all users on the LAN are allowed non-restricted access to the WAN. When you configure a LAN to WAN rule, you in essence want to limit some or all users from accessing certain services on the WAN. **WAN to LAN Rules**

The default rule for WAN to LAN traffic blocks all incoming connections (WAN to LAN). If you wish to allow certain WAN users to have access to your LAN, you will need to create custom rules to allow it.

### 15.4.2 Alerts

Alerts are reports on events, such as attacks, that you may want to know about right away. You can choose to generate an alert when a rule is matched in the **Edit Rule** screen (see [Figure 142 on page 252](#)). When an event generates an alert, a message can be immediately sent to an e-mail account that you specify in the **Log Settings** screen. Refer to [Chapter 27 on page 387](#) for details.

## 15.5 General Firewall Policy

Click **Security > Firewall** to display the following screen. Activate the firewall by selecting the **Active Firewall** check box as seen in the following screen.

Refer to [Section 14.1 on page 233](#) for more information.

**Figure 140** Firewall: General

Packet Direction	Default Action	Log
WAN to LAN	Drop	<input checked="" type="checkbox"/>
LAN to WAN	Permit	<input checked="" type="checkbox"/>
WAN to WAN / Router	Drop	<input checked="" type="checkbox"/>
LAN to LAN / Router	Permit	<input type="checkbox"/>

The following table describes the labels in this screen.

**Table 91** Firewall: General

LABEL	DESCRIPTION
Active Firewall	Select this check box to activate the firewall. The ZyXEL Device performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Bypass Triangle Route	Select this check box to have the ZyXEL Device firewall permit the use of triangle route topology on the network. See the appendix for more on triangle route topology.  Note: Allowing asymmetrical routes may let traffic from the WAN go directly to a LAN computer without passing through the router.
Packet Direction	This is the direction of travel of packets ( <b>LAN to LAN / Router, LAN to WAN, WAN to WAN / Router, WAN to LAN</b> ).  Firewall rules are grouped based on the direction of travel of packets to which they apply. For example, <b>LAN to LAN / Router</b> means packets traveling from a computer/subnet on the LAN to either another computer/subnet on the LAN interface of the ZyXEL Device or the ZyXEL Device itself.
Default Action	Use the drop-down list boxes to select the default action that the firewall is take on packets that are traveling in the selected direction and do not match any of the firewall rules.  Select <b>Drop</b> to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. Select <b>Reject</b> to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender. Select <b>Permit</b> to allow the passage of the packets.
Log	Select the check box to create a log (when the above action is taken) for packets that are traveling in the selected direction and do not match any of your customized rules.
Expand...	Click this button to display more information.
Basic...	Click this button to display less information.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

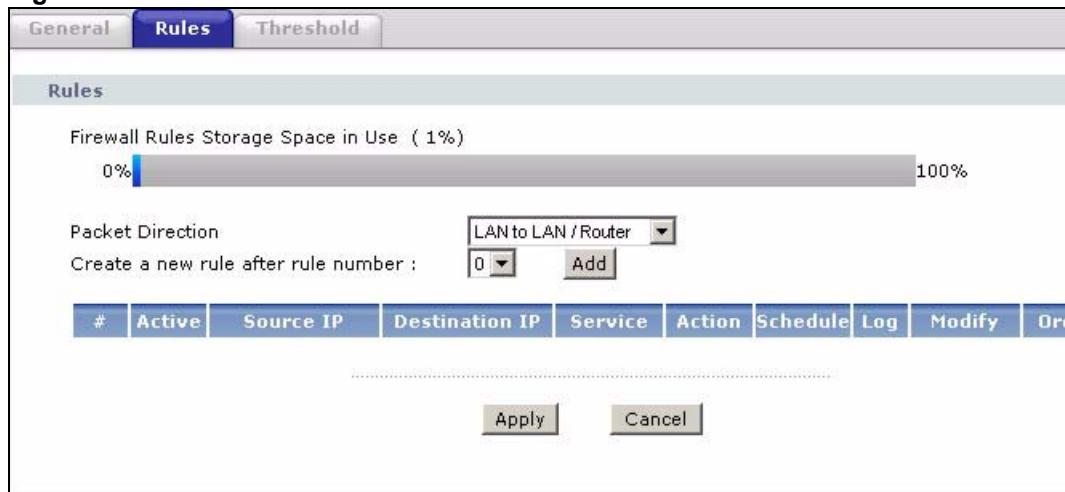
## 15.6 Firewall Rules Summary



The ordering of your rules is very important as rules are applied in turn.

Refer to [Section 14.1 on page 233](#) for more information.

Click **Security > Firewall > Rules** to bring up the following screen. This screen displays a list of the configured firewall rules. Note the order in which the rules are listed.

**Figure 141** Firewall Rules

The following table describes the labels in this screen.

**Table 92** Firewall Rules

LABEL	DESCRIPTION
Firewall Rules Storage Space in Use	This read-only bar shows how much of the ZyXEL Device's memory for recording firewall rules it is currently using. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red.
Packet Direction	Use the drop-down list box to select a direction of travel of packets for which you want to configure firewall rules.
Create a new rule after rule number	Select an index number and click <b>Add</b> to add a new firewall rule after the selected index number. For example, if you select "6", your new rule becomes number 7 and the previous rule 7 (if there is one) becomes rule 8.
	The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings in the <b>General</b> screen.
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
Active	This field displays whether a firewall is turned on or not. Select the check box to enable the rule. Clear the check box to disable the rule.
Source IP	This drop-down list box displays the source addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to <b>Any</b> .
Destination IP	This drop-down list box displays the destination addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to <b>Any</b> .
Service	This drop-down list box displays the services to which this firewall rule applies. See <a href="#">Appendix E on page 475</a> for more information.
Action	This field displays whether the firewall silently discards packets ( <b>Drop</b> ), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender ( <b>Reject</b> ) or allows the passage of packets ( <b>Permit</b> ).
Schedule	This field tells you whether a schedule is specified ( <b>Yes</b> ) or not ( <b>No</b> ).
Log	This field shows you whether a log is created when packets match this rule ( <b>Yes</b> ) or not ( <b>No</b> ).

**Table 92** Firewall Rules (continued)

LABEL	DESCRIPTION
Modify	Click the Edit icon to go to the screen where you can edit the rule. Click the Remove icon to delete an existing firewall rule. A window displays asking you to confirm that you want to delete the firewall rule. Note that subsequent firewall rules move up by one when you take this action.
Order	Click the Move icon to display the <b>Move the rule to</b> field. Type a number in the <b>Move the rule to</b> field and click the <b>Move</b> button to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

### 15.6.1 Configuring Firewall Rules

Refer to [Section 14.1 on page 233](#) for more information.

In the **Rules** screen, select an index number and click **Add** or click a rule's **Edit** icon to display this screen and refer to the following table for information on the labels.

**Figure 142** Firewall: Edit Rule

**Edit Rule 2**

Active  
Action for Matched Packets: **Permit**

**Source Address**

Address Type: Any Address  
Start IP: 0.0.0.0  
Address: 0.0.0.0  
End IP: 0.0.0.0  
Address: 0.0.0.0  
Subnet Mask: 0.0.0.0

Add >> Edit << Delete

Source Address List: Any

**Destination Address**

Address Type: Any Address  
Start IP: 0.0.0.0  
Address: 0.0.0.0  
End IP: 0.0.0.0  
Address: 0.0.0.0  
Subnet Mask: 0.0.0.0

Add >> Edit << Delete

Destination Address List: Any

**Service**

Available Services: Any(All), Any(ICMP), AIMNEW-ICQ(TCP:5190), AUTH(TCP:113), BGP(TCP:179)

Add >> Remove

Selected Services: Any(UDP), Any(TCP)

[Edit Customized Services](#)

**Schedule**

Day to Apply:  
 Everyday  
 Sun  Mon  Tue  Wed  Thu  Fri  Sat

Time of Day to Apply : (24-Hour Format)  
 All day  
Start  hour  minute End  hour  minute

Log  
 Log Packet Detail Information.

Alert  
 Send Alert Message to Administrator When Matched.

Apply Cancel

The following table describes the labels in this screen.

**Table 93** Firewall: Edit Rule

LABEL	DESCRIPTION
Active	Select this option to enable this firewall rule.
Action for Matched Packet	Use the drop-down list box to select whether to discard ( <b>Drop</b> ), deny and send an ICMP destination-unreachable message to the sender of ( <b>Reject</b> ) or allow the passage of ( <b>Permit</b> ) packets that match this rule.

**Table 93** Firewall: Edit Rule (continued)

LABEL	DESCRIPTION
Source/Destination Address	
Address Type	Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (for instance, 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: <b>Single Address</b> , <b>Range Address</b> , <b>Subnet Address</b> and <b>Any Address</b> .
Start IP Address	Enter the single IP address or the starting IP address in a range here.
End IP Address	Enter the ending IP address in a range here.
Subnet Mask	Enter the subnet mask here, if applicable.
Add >>	Click <b>Add &gt;&gt;</b> to add a new address to the <b>Source or Destination Address</b> box. You can add multiple addresses, ranges of addresses, and/or subnets.
Edit <<	To edit an existing source or destination address, select it from the box and click <b>Edit &lt;&lt;</b> .
Delete	Highlight an existing source or destination address from the <b>Source or Destination Address</b> box above and click <b>Delete</b> to remove it.
Services	
Available/ Selected Services	Please see <a href="#">Appendix E on page 475</a> for more information on services available. Highlight a service from the <b>Available Services</b> box on the left, then click <b>Add &gt;&gt;</b> to add it to the <b>Selected Services</b> box on the right. To remove a service, highlight it in the <b>Selected Services</b> box on the right, then click <b>Remove</b> .
Edit Customized Service	Click the <b>Edit Customized Services</b> link to bring up the screen that you use to configure a new custom service that is not in the predefined list of services.
Schedule	
Day to Apply	Select everyday or the day(s) of the week to apply the rule.
Time of Day to Apply (24-Hour Format)	Select <b>All Day</b> or enter the start and end times in the hour-minute format to apply the rule.
Log	
Log Packet Detail Information	This field determines if a log for packets that match the rule is created or not. Go to the <b>Log Settings</b> page and select the <b>Access Control</b> logs category to have the ZyXEL Device record these logs.
Alert	
Send Alert Message to Administrator When Matched	Select the check box to have the ZyXEL Device generate an alert when the rule is matched.
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 15.6.2 Customized Services

Configure customized services and port numbers not predefined by the ZyXEL Device. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. See [Appendix E on page 475](#) for some examples. Click the **Edit Customized Services** link while editing a firewall rule to configure a custom service port. This displays the following screen.

Refer to [Section 14.1 on page 233](#) for more information.

**Figure 143** Firewall: Customized Services

Customized Services			
No.	Name	Protocol	Port
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

Back

The following table describes the labels in this screen.

**Table 94** Customized Services

LABEL	DESCRIPTION
No.	This is the number of your customized port. Click a rule's number of a service to go to the <b>Firewall Customized Services Config</b> screen to configure or edit a customized service.
Name	This is the name of your customized service.
Protocol	This shows the IP protocol (TCP, UDP or TCP/UDP) that defines your customized service.
Port	This is the port number or range that defines your customized service.
Back	Click <b>Back</b> to return the <b>Firewall Edit Rule</b> screen.

## 15.6.3 Configuring a Customized Service

Click a rule number in the **Firewall Customized Services** screen to create a new custom port or edit an existing one. This action displays the following screen.

Refer to [Section 14.1 on page 233](#) for more information.

**Figure 144** Firewall: Configure Customized Services

The following table describes the labels in this screen.

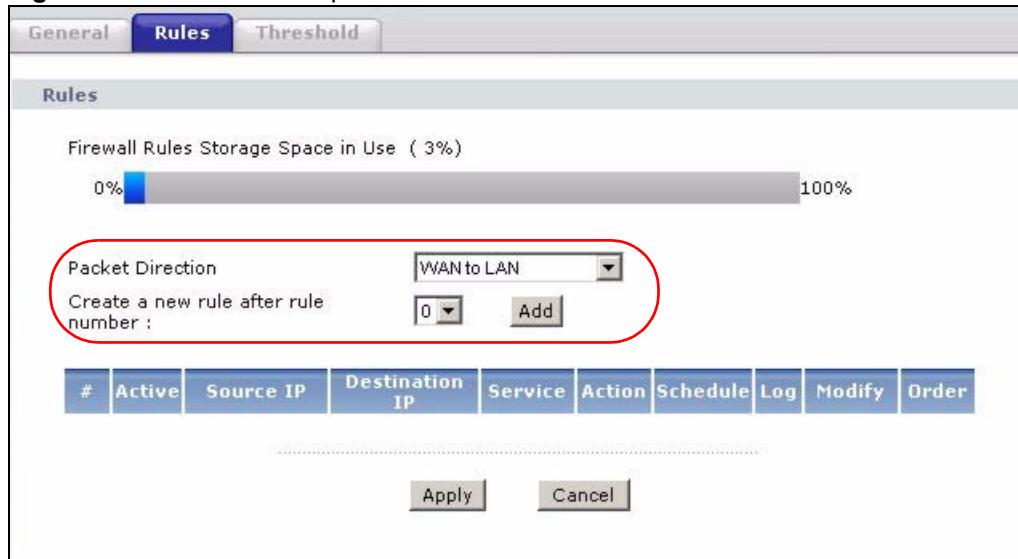
**Table 95** Firewall: Configure Customized Services

LABEL	DESCRIPTION
Service Name	Type a unique name for your custom port.
Service Type	Choose the IP port ( <b>TCP</b> , <b>UDP</b> or <b>TCP/UDP</b> ) that defines your customized port from the drop down list box.
Port Configuration	
Type	Click <b>Single</b> to specify one port only or <b>Range</b> to specify a span of ports that define your customized service.
Port Number	Type a single port number or the range of port numbers that define your customized service.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to return to the previously saved settings.
Delete	Click <b>Delete</b> to delete the current rule.

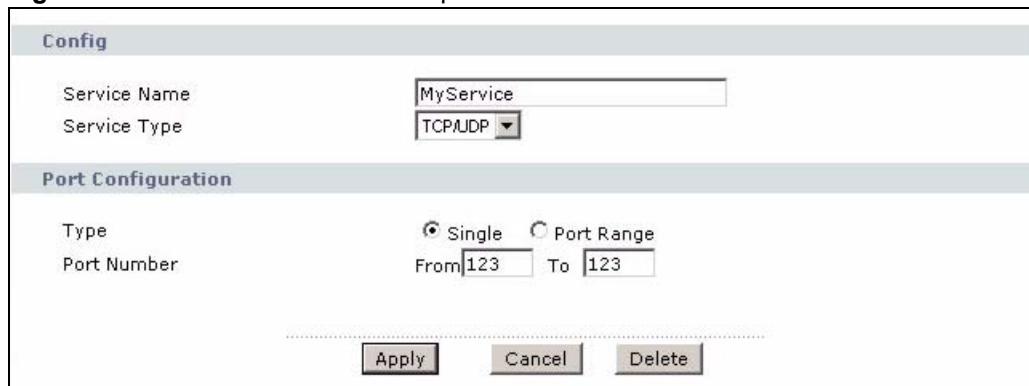
## 15.7 Example Firewall Rule

The following Internet firewall rule example allows a hypothetical “MyService” connection from the Internet.

- 1 Click **Security > Firewall > Rules**.
- 2 Select **WAN to LAN** in the **Packet Direction** field.

**Figure 145** Firewall Example: Rules

- 3 In the **Rules** screen, select the index number after that you want to add the rule. For example, if you select “6”, your new rule becomes number 7 and the previous rule 7 (if there is one) becomes rule 8.
- 4 Click **Add** to display the firewall rule configuration screen.
- 5 In the **Edit Rule** screen, click the **Edit Customized Services** link to open the **Customized Service** screen.
- 6 Click an index number to display the **Customized Services Config** screen and configure the screen as follows and click **Apply**.

**Figure 146** Edit Custom Port Example

- 7 Select **Any** in the **Destination Address** box and then click **Delete**.
- 8 Configure the destination address screen as follows and click **Add**.

**Figure 147** Firewall Example: Edit Rule: Destination Address

The screenshot shows the 'Edit Rule 1' configuration window. At the top, there is a checkbox labeled 'Active' which is checked, and a dropdown menu labeled 'Action for Matched Packets:' with the value 'Permit'.  
**Source Address:** This section contains fields for 'Address Type' (set to 'Any Address'), 'Start IP' (0.0.0.0), 'End IP' (0.0.0.0), 'Address' (0.0.0.0), and 'Subnet Mask' (0.0.0.0). To the right, there is a 'Source Address List' containing the entry 'Any', with buttons for 'Add >>', 'Edit <<', and 'Delete'.  
**Destination Address:** This section contains fields for 'Address Type' (set to 'Range Address'), 'Start IP' (10.0.0.10), 'End IP' (10.0.0.15), 'Address' (10.0.0.10 - 10.0.0.15), and 'Subnet Mask' (0.0.0.0). To the right, there is a 'Destination Address List' containing the entry '10.0.0.10 - 10.0.0.15', with buttons for 'Add >>', 'Edit <<', and 'Delete'.

- 9** Use the **Add >>** and **Remove** buttons between **Available Services** and **Selected Services** list boxes to configure it as follows. Click **Apply** when you are done.



Custom services show up with an '\*' before their names in the **Services** list box and the **Rules** list box.

**Figure 148** Firewall Example: Edit Rule: Select Customized Services

**Edit Rule 2**

Active  
Action for Matched Packets: Permit

**Source Address**

Address Type: Any Address  
Start IP: 0.0.0.0  
Address: 0.0.0.0  
End IP: 0.0.0.0  
Address: 0.0.0.0  
Subnet Mask: 0.0.0.0

Add >> Edit << Delete

Source Address List: Any

**Destination Address**

Address Type: Range Address  
Start IP: 10.0.0.10  
Address: 10.0.0.10  
End IP: 10.0.0.15  
Address: 10.0.0.15  
Subnet Mask: 0.0.0.0

Add >> Edit << Delete

Destination Address List: 10.0.0.10 - 10.0.0.15

**Service**

Available Services: Any(All), Any(ICMP), AIM/NEW-ICQ(TCP:5190), AUTH(TCP:113), BGP(TCP:179)

Add >> Remove

Selected Services: \*MyService(TCP/UDP:123)

[Edit Customized Services](#)

**Schedule**

Day to Apply:  
 Everyday  
 Sun  Mon  Tue  Wed  Thu  Fri  Sat

Time of Day to Apply : (24-Hour Format)  
 All day  
Start [ ] hour [ ] minute   End [ ] hour [ ] minute

Log  
 Log Packet Detail Information.

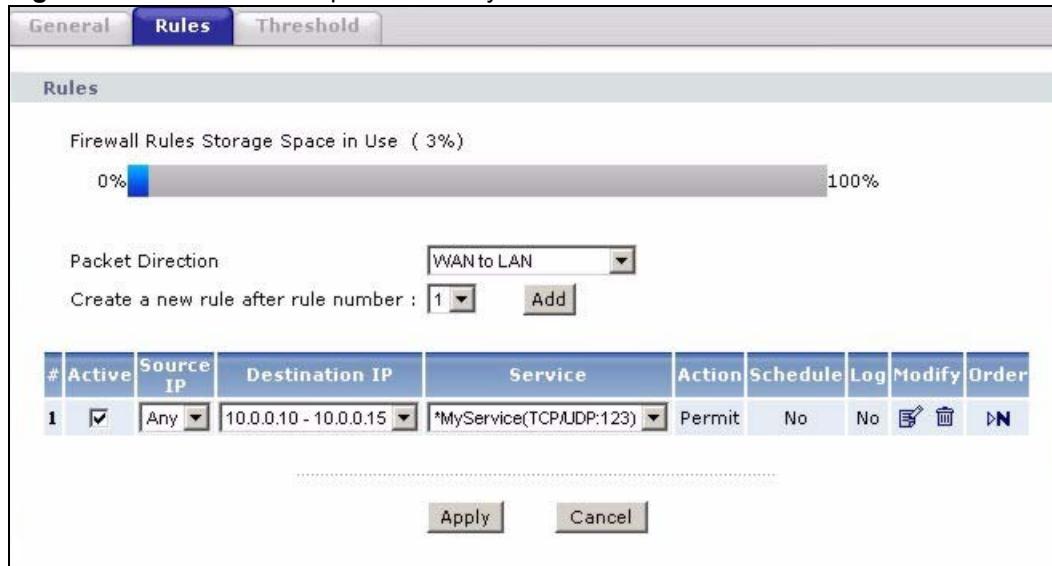
Alert  
 Send Alert Message to Administrator When Matched.

.....

**Buttons:** Apply (highlighted with a red circle), Cancel

On completing the configuration procedure for this Internet firewall rule, the **Rules** screen should look like the following.

Rule 1 allows a “MyService” connection from the WAN to IP addresses 10.0.0.10 through 10.0.0.15 on the LAN.

**Figure 149** Firewall Example: Rules: MyService

## 15.8 DoS Thresholds

For DoS attacks, the ZyXEL Device uses thresholds to determine when to drop sessions that do not become fully established. These thresholds apply globally to all sessions.

You can use the default threshold values, or you can change them to values more suitable to your security requirements.

Refer to [Section 15.8.3 on page 260](#) to configure thresholds.

### 15.8.1 Threshold Values

Tune these parameters when something is not working and after you have checked the firewall counters. These default values should work fine for most small offices. Factors influencing choices for threshold values are:

- The maximum number of opened sessions.
- The minimum capacity of server backlog in your LAN network.
- The CPU power of servers in your LAN network.
- Network bandwidth.
- Type of traffic for certain servers.

If your network is slower than average for any of these factors (especially if you have servers that are slow or handle many tasks and are often busy), then the default values should be reduced.

You should make any changes to the threshold values before you continue configuring firewall rules.

## 15.8.2 Half-Open Sessions

An unusually high number of half-open sessions (either an absolute number or measured as the arrival rate) could indicate that a Denial of Service attack is occurring. For TCP, "half-open" means that the session has not reached the established state—the TCP three-way handshake has not yet been completed (see [Figure 136 on page 236](#)). For UDP, "half-open" means that the firewall has detected no return traffic.

The ZyXEL Device measures both the total number of existing half-open sessions and the [rate](#) of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (**max-incomplete high**), the ZyXEL Device starts deleting half-open sessions as required to accommodate new connection requests. The ZyXEL Device continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (**max-incomplete low**).

When the rate of new connection attempts rises above a threshold (**one-minute high**), the ZyXEL Device starts deleting half-open sessions as required to accommodate new connection requests. The ZyXEL Device continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (**one-minute low**). The rate is the number of new attempts detected in the last one-minute sample period.

### 15.8.2.1 TCP Maximum Incomplete and Blocking Time

An unusually high number of half-open sessions with the same destination host address could indicate that a Denial of Service attack is being launched against the host.

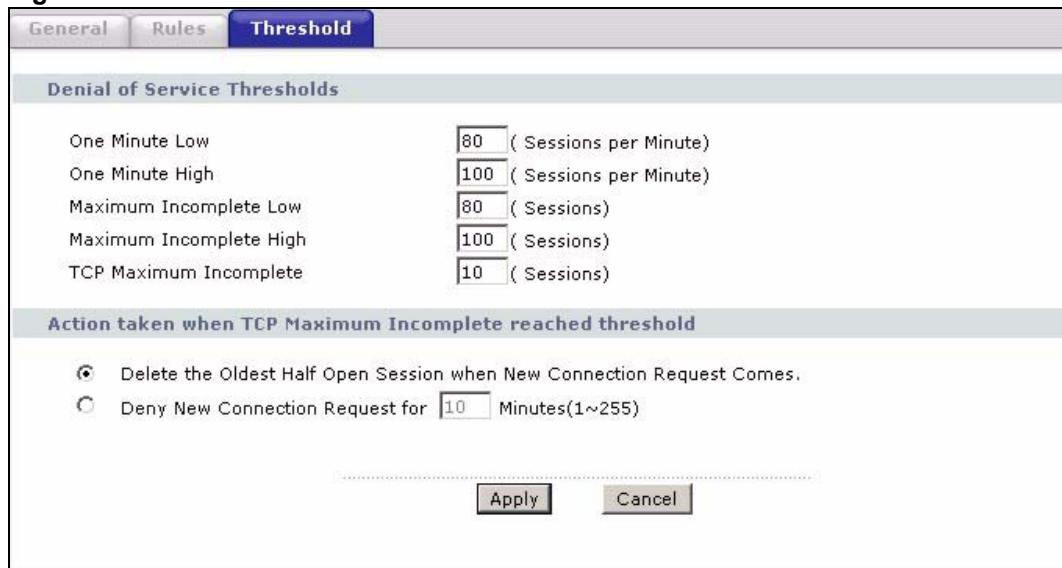
Whenever the number of half-open sessions with the same destination host address rises above a threshold (**TCP Maximum Incomplete**), the ZyXEL Device starts deleting half-open sessions according to one of the following methods:

- If the **Blocking Time** timeout is 0 (the default), then the ZyXEL Device deletes the oldest existing half-open session for the host for every new connection request to the host. This ensures that the number of half-open sessions to a given host will never exceed the threshold.
- If the **Blocking Time** timeout is greater than 0, then the ZyXEL Device blocks all new connection requests to the host giving the server time to handle the present connections. The ZyXEL Device continues to block all new connection requests until the **Blocking Time** expires.

## 15.8.3 Configuring Firewall Thresholds

The ZyXEL Device also sends alerts whenever **TCP Maximum Incomplete** is exceeded. The global values specified for the threshold and timeout apply to all TCP connections.

Click **Firewall**, and **Threshold** to bring up the next screen.

**Figure 150** Firewall: Threshold

The following table describes the labels in this screen.

**Table 96** Firewall: Threshold

LABEL	DESCRIPTION	DEFAULT VALUES
Denial of Service Thresholds		
One Minute Low	This is the rate of new half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyXEL Device continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number.	80 existing half-open sessions.
One Minute High	This is the rate of new half-open sessions that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the ZyXEL Device deletes half-open sessions as required to accommodate new connection attempts.	100 half-open sessions per minute. The above numbers cause the ZyXEL Device to start deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 80 session establishment attempts have been detected in the last minute.
Maximum Incomplete Low	This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyXEL Device continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number.	80 existing half-open sessions.

**Table 96** Firewall: Threshold (continued)

LABEL	DESCRIPTION	DEFAULT VALUES
Maximum Incomplete High	This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the ZyXEL Device deletes half-open sessions as required to accommodate new connection requests. Do not set <b>Maximum Incomplete High</b> to lower than the current <b>Maximum Incomplete Low</b> number.	100 existing half-open sessions. The above values causes the ZyXEL Device to start deleting half-open sessions when the number of existing half-open sessions rises above 100, and to stop deleting half-open sessions with the number of existing half-open sessions drops below 80.
TCP Maximum Incomplete	This is the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 256. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth.	30 existing half-open TCP sessions.
Action taken when the TCP Maximum Incomplete reached threshold		
Delete the Oldest Half Open Session when New Connection Request Comes.	Select this radio button to clear the oldest half open session when a new connection request comes.	
Deny New Connection Request for	Select this radio button and specify for how long the ZyXEL Device should block new connection requests when <b>TCP Maximum Incomplete</b> is reached. Enter the length of blocking time in minutes (between 1 and 256).	
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.	
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.	

## 15.9 Firewall Commands

The following describes the firewall commands. See the Command Interpreter appendix for information on the command structure. Each of these commands must be preceded by `sys firewall` when you use them. For example, type `sys firewall active yes` to turn on the firewall.

**Table 97** Sys Firewall Commands

COMMAND	DESCRIPTION	
acl		
	disp	Displays ACLs or a specific ACL set # and rule #.
active	<yes   no>	Active firewall or deactivate firewall Enables/disables the firewall.
cnt		

**Table 97** Sys Firewall Commands

COMMAND		DESCRIPTION
	disp	Displays the firewall log type and count.
	clear	Clears the firewall log count.
pktdump		Dumps the last 64 bytes of packets that the firewall has dropped.
dynamicrule	display	Displays the firewall's dynamic rules.
tcprst		
	rst	Turns TCP reset sending on/off.
	rst113	Turns TCP reset sending for port 113 on/off.
	display	Displays the TCP reset sending settings.
icmp		This rule is not in use.
dos		
	smtp	Enables/disables the SMTP DoS defender.
	display	Displays the SMTP DoS defender setting.
	ignore	Sets if the firewall will ignore DoS attacks on the lan/wan.
ignore		
	dos	Sets if the firewall will ignore DoS attacks on the lan/wan.
	triangle	Sets if the firewall will ignore triangle route packets on the lan/wan.



# Content Filtering

This chapter covers how to configure content filtering.

## 16.1 Content Filtering Overview

Internet content filtering allows you to create and enforce Internet access policies tailored to your needs. Content filtering gives you the ability to block web sites that contain key words (that you specify) in the URL. You can set a schedule for when the ZyXEL Device performs content filtering. You can also specify trusted IP addresses on the LAN for which the ZyXEL Device will not perform content filtering.

## 16.2 Configuring Keyword Blocking

Use this screen to block sites containing certain keywords in the URL. For example, if you enable the keyword "bad", the ZyXEL Device blocks all sites containing this keyword including the URL <http://www.website.com/bad.html>, even if it is not included in the Filter List.

To have your ZyXEL Device block Web sites containing keywords in their URLs, click **Security > Content Filter**. The screen appears as shown.

**Figure 151** Content Filter: Keyword

The screenshot shows a software interface for managing content filtering rules. At the top, there is a navigation bar with three tabs: 'Keyword' (which is selected and highlighted in blue), 'Schedule', and 'Trusted'. Below the tabs, the main area is titled 'Keyword'. A checkbox labeled 'Active Keyword Blocking' is checked. Underneath, a section titled 'Block Websites that contain these keywords in the URL :' contains a single word 'bad' listed in a text input field. At the bottom of this section are two buttons: 'Delete' and 'Clear All'. Below this is a search bar with a placeholder 'Keyword' and an 'Add Keyword' button. At the very bottom of the screen are two more buttons: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

**Table 98** Content Filter: Keyword

LABEL	DESCRIPTION
Active Keyword Blocking	Select this check box to enable this feature.
Block Websites that contain these keywords in the URL:	This box contains the list of all the keywords that you have configured the ZyXEL Device to block.
Delete	Highlight a keyword in the box and click <b>Delete</b> to remove it.
Clear All	Click <b>Clear All</b> to remove all of the keywords from the list.
Keyword	Type a keyword in this field. You may use any character (up to 127 characters). Wildcards are not allowed.
Add Keyword	Click <b>Add Keyword</b> after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to return to the previously saved settings.

## 16.3 Configuring the Schedule

Use this screen to set the days and times for the ZyXEL Device to perform content filtering. Click **Security > Content Filter > Schedule**. The screen appears as shown.

**Figure 152** Content Filter: Schedule

Keyword	Schedule	Trusted																																
<p><b>Schedule</b></p> <p><input type="checkbox"/> Block Everyday  <input checked="" type="checkbox"/> Edit Daily to Block</p> <table border="1"> <thead> <tr> <th></th> <th>Active</th> <th>Start Time</th> <th>End Time</th> </tr> </thead> <tbody> <tr> <td>Monday</td> <td><input type="checkbox"/></td> <td>0 hr 0 min</td> <td>0 hr 0 min</td> </tr> <tr> <td>Tuesday</td> <td><input type="checkbox"/></td> <td>0 hr 0 min</td> <td>0 hr 0 min</td> </tr> <tr> <td>Wednesday</td> <td><input type="checkbox"/></td> <td>0 hr 0 min</td> <td>0 hr 0 min</td> </tr> <tr> <td>Thursday</td> <td><input type="checkbox"/></td> <td>0 hr 0 min</td> <td>0 hr 0 min</td> </tr> <tr> <td>Friday</td> <td><input type="checkbox"/></td> <td>0 hr 0 min</td> <td>0 hr 0 min</td> </tr> <tr> <td>Saturday</td> <td><input type="checkbox"/></td> <td>0 hr 0 min</td> <td>0 hr 0 min</td> </tr> <tr> <td>Sunday</td> <td><input type="checkbox"/></td> <td>0 hr 0 min</td> <td>0 hr 0 min</td> </tr> </tbody> </table> <p>.....</p> <p style="text-align: center;"><b>Apply</b>    <b>Cancel</b></p>				Active	Start Time	End Time	Monday	<input type="checkbox"/>	0 hr 0 min	0 hr 0 min	Tuesday	<input type="checkbox"/>	0 hr 0 min	0 hr 0 min	Wednesday	<input type="checkbox"/>	0 hr 0 min	0 hr 0 min	Thursday	<input type="checkbox"/>	0 hr 0 min	0 hr 0 min	Friday	<input type="checkbox"/>	0 hr 0 min	0 hr 0 min	Saturday	<input type="checkbox"/>	0 hr 0 min	0 hr 0 min	Sunday	<input type="checkbox"/>	0 hr 0 min	0 hr 0 min
	Active	Start Time	End Time																															
Monday	<input type="checkbox"/>	0 hr 0 min	0 hr 0 min																															
Tuesday	<input type="checkbox"/>	0 hr 0 min	0 hr 0 min																															
Wednesday	<input type="checkbox"/>	0 hr 0 min	0 hr 0 min																															
Thursday	<input type="checkbox"/>	0 hr 0 min	0 hr 0 min																															
Friday	<input type="checkbox"/>	0 hr 0 min	0 hr 0 min																															
Saturday	<input type="checkbox"/>	0 hr 0 min	0 hr 0 min																															
Sunday	<input type="checkbox"/>	0 hr 0 min	0 hr 0 min																															

The following table describes the labels in this screen.

**Table 99** Content Filter: Schedule

LABEL	DESCRIPTION
Schedule	Select <b>Block Everyday</b> to make the content filtering active everyday. Otherwise, select <b>Edit Daily to Block</b> and configure which days of the week (or everyday) and which time of the day you want the content filtering to be active.
Active	Select the check box to have the content filtering to be active on the selected day.
Start Time	Enter the time when you want the content filtering to take effect in hour-minute format.
End Time	Enter the time when you want the content filtering to stop in hour-minute format.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to return to the previously saved settings.

## 16.4 Configuring Trusted Computers

Use this screen to exclude a range of users on the LAN from content filtering on your ZyXEL Device. Click **Security > Content Filter > Trusted**. The screen appears as shown.

**Figure 153** Content Filter: Trusted

The screenshot shows a software interface for configuring trusted users. At the top, there are three tabs: 'Keyword', 'Schedule', and 'Trusted'. The 'Trusted' tab is currently selected and highlighted in blue. Below the tabs, the title 'Trusted User IP Range' is displayed. Under this title, there are two input fields: 'Start IP Address' containing '0.0.0.0' and 'End IP Address' also containing '0.0.0.0'. At the bottom of the screen, there are two buttons: 'Apply' on the left and 'Cancel' on the right.

The following table describes the labels in this screen.

**Table 100** Content Filter: Trusted

LABEL	DESCRIPTION
Trusted User IP Range	
Start IP Address	Type the single IP address of a computer (or the beginning IP address of a specific range of computers) on the LAN that you want to exclude from content filtering.
End IP Address	Type the ending IP address of a specific range of users on your LAN that you want to exclude from content filtering. Leave this field blank if you want to exclude an individual computer.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to return to the previously saved settings.



# Introduction to IPSec

This chapter introduces the basics of IPSec VPNs.

## 17.1 VPN Overview

A VPN (Virtual Private Network) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing technologies/services used to transport traffic over the Internet or any insecure network that uses the TCP/IP protocol suite for communication.

### 17.1.1 IPSec

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

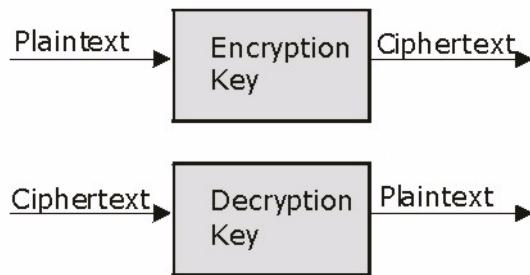
### 17.1.2 Security Association

A Security Association (SA) is a contract between two parties indicating what security parameters, such as keys and algorithms they will use.

### 17.1.3 Other Terminology

#### 17.1.3.1 Encryption

Encryption is a mathematical operation that transforms data from "plaintext" (readable) to "ciphertext" (scrambled text) using a "key". The key and clear text are processed by the encryption operation, which leads to the data scrambling that makes encryption secure. Decryption is the opposite of encryption: it is a mathematical operation that transforms "ciphertext" to plaintext. Decryption also requires a key.

**Figure 154** Encryption and Decryption

#### 17.1.3.2 Data Confidentiality

The IPSec sender can encrypt packets before transmitting them across a network.

#### 17.1.3.3 Data Integrity

The IPSec receiver can validate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.

#### 17.1.3.4 Data Origin Authentication

The IPSec receiver can verify the source of IPSec packets. This service depends on the data integrity service.

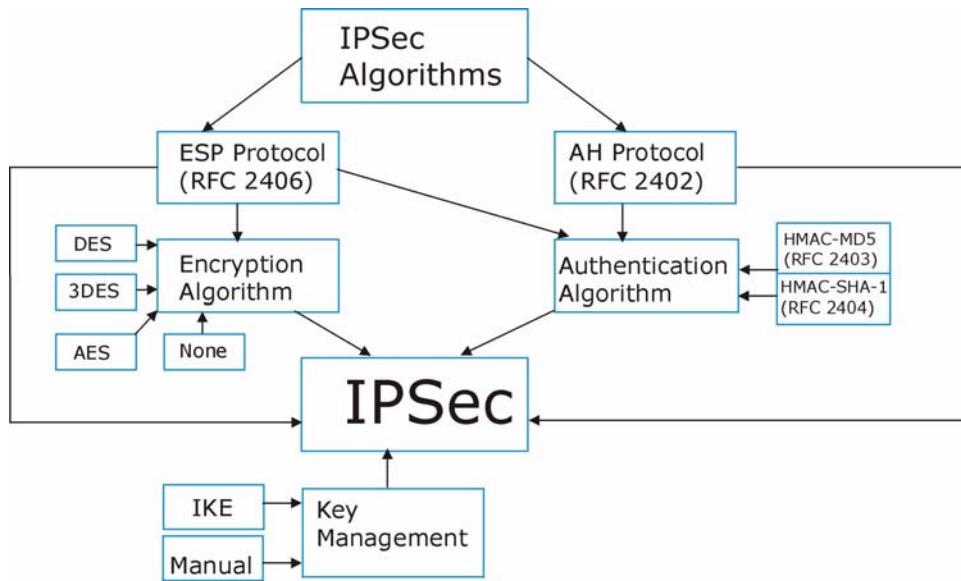
### 17.1.4 VPN Applications

The ZyXEL Device supports the following VPN applications.

- Linking Two or More Private Networks Together  
Connect branch offices and business partners over the Internet with significant cost savings and improved performance when compared to leased lines between sites.
- Accessing Network Resources When NAT Is Enabled  
When NAT is enabled, remote users are not able to access hosts on the LAN unless the host is designated a public LAN server for that specific protocol. Since the VPN tunnel terminates inside the LAN, remote users will be able to access all computers that use private IP addresses on the LAN.
- Unsupported IP Applications  
A VPN tunnel may be created to add support for unsupported emerging IP applications.

## 17.2 IPSec Architecture

The overall IPSec architecture is shown as follows.

**Figure 155** IPSec Architecture

### 17.2.1 IPSec Algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard) and Triple DES algorithms.

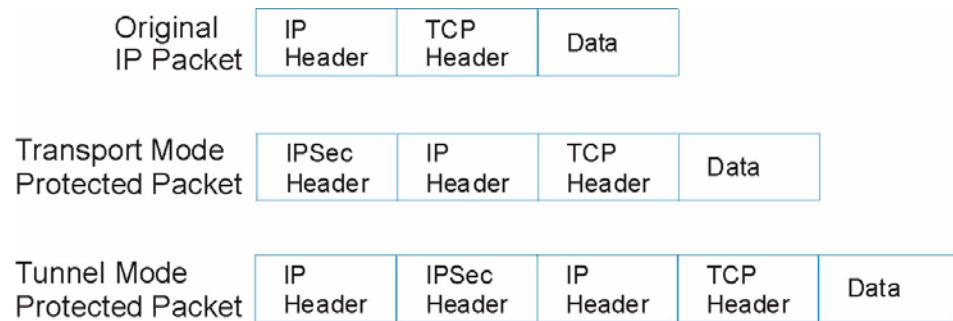
The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404), provide an authentication mechanism for the **AH** and **ESP** protocols. Please see [Section 18.2 on page 275](#) for more information.

### 17.2.2 Key Management

Key management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN.

## 17.3 Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode.

**Figure 156** Transport and Tunnel Mode IPSec Encapsulation

### 17.3.1 Transport Mode

**Transport** mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP).

With **ESP**, protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.

With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process.

### 17.3.2 Tunnel Mode

**Tunnel** mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for gateway to gateway and host to gateway communications. **Tunnel** mode communications have two sets of IP headers:

- **Outside header:** The outside IP header contains the destination IP address of the VPN gateway.
- **Inside header:** The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

## 17.4 IPSec and NAT

Read this section if you are running IPSec on a host computer behind the ZyXEL Device.

NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN gateway, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

**Tunnel** mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device.

**Transport** mode **ESP** with authentication is not compatible with NAT.

**Table 101** VPN and NAT

SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	N
ESP	Tunnel	Y



# VPN Screens

This chapter introduces the VPN screens. See [Chapter 27 on page 387](#) for information on viewing logs and the appendix for IPSec log descriptions.

## 18.1 VPN/IPSec Overview

Use the screens documented in this chapter to configure rules for VPN connections and manage VPN connections.

## 18.2 IPSec Algorithms

The **ESP** and **AH** protocols are necessary to create a Security Association (SA), the foundation of an IPSec VPN. An SA is built from the authentication provided by the **AH** and **ESP** protocols. The primary function of key management is to establish and maintain the SA between systems. Once the SA is established, the transport of data may commence.

### 18.2.1 AH (Authentication Header) Protocol

**AH** protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the **ESP** was designed.

In applications where confidentiality is not required or not sanctioned by government encryption restrictions, an **AH** can be employed to ensure integrity. This type of implementation does not protect the information from dissemination but will allow for verification of the integrity of the information and authentication of the originator.

### 18.2.2 ESP (Encapsulating Security Payload) Protocol

The **ESP** protocol (RFC 2406) provides encryption as well as the services offered by **AH**. **ESP** authenticating properties are limited compared to the **AH** due to the non-inclusion of the IP header information during the authentication process. However, **ESP** is sufficient if only the upper layer protocols need to be authenticated.

An added feature of the **ESP** is payload padding, which further protects communications by concealing the size of the packet being transmitted.

**Table 102** AH and ESP

	<b>ESP</b>	<b>AH</b>
<b>ENCRYPTION</b>	<b>DES</b> (default) Data Encryption Standard (DES) is a widely used method of data encryption using a private (secret) key. DES applies a 56-bit key to each 64-bit block of data.	<b>MD5</b> (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
	<b>3DES</b> Triple DES (3DES) is a variant of DES, which iterates three times with three separate keys ( $3 \times 56 = 168$ bits), effectively doubling the strength of DES.	<b>SHA1</b> SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
	<b>AES</b> Advanced Encryption Standard is a newer method of data encryption that also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data. AES is faster than 3DES.	
	Select <b>NULL</b> to set up a phase 2 tunnel without encryption.	
<b>AUTHENTICATION</b>	<b>MD5</b> (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.	<b>MD5</b> (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
	<b>SHA1</b> SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.	<b>SHA1</b> SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
	Select <b>MD5</b> for minimal security and <b>SHA1</b> for maximum security.	

## 18.3 My IP Address

My IP Address is the WAN IP address of the ZyXEL Device. The ZyXEL Device has to rebuild the VPN tunnel if My IP Address changes after setup.

The following applies if this field is configured as **0.0.0.0**:

- The ZyXEL Device uses the current ZyXEL Device WAN IP address (static or dynamic) to set up the VPN tunnel.
- If the WAN connection goes down, the ZyXEL Device uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See [Chapter 7 on page 101](#) for details on dial backup and traffic redirect.

## 18.4 Secure Gateway Address

**Secure Gateway Address** is the WAN IP address or domain name of the remote IPSec router (secure gateway).

If the remote secure gateway has a static WAN IP address, enter it in the **Secure Gateway Address** field. You may alternatively enter the remote secure gateway's domain name (if it has one) in the **Secure Gateway Address** field.

You can also enter a remote secure gateway's domain name in the **Secure Gateway Address** field if the remote secure gateway has a dynamic WAN IP address and is using DDNS. The ZyXEL Device has to rebuild the VPN tunnel each time the remote secure gateway's WAN IP address changes (there may be a delay until the DDNS servers are updated with the remote gateway's new WAN IP address).

#### 18.4.1 Dynamic Secure Gateway Address

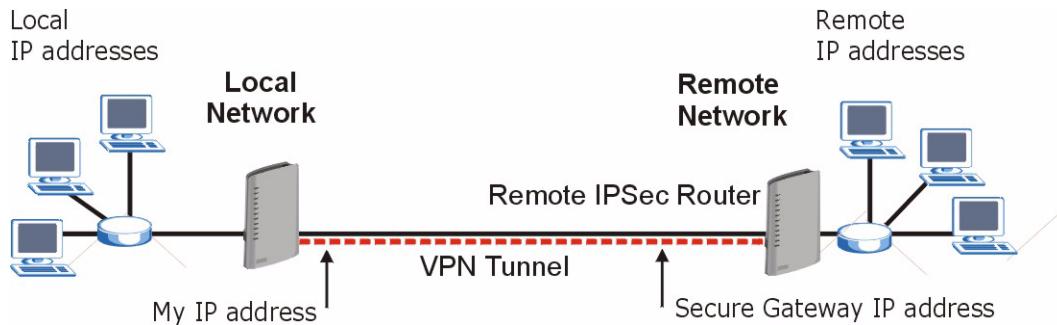
If the remote secure gateway has a dynamic WAN IP address and does not use DDNS, enter 0.0.0.0 as the secure gateway's address. In this case only the remote secure gateway can initiate SAs. This may be useful for telecommuters initiating a VPN tunnel to the company network (see [Section 18.18 on page 297](#) for configuration examples).

The Secure Gateway IP Address may be configured as 0.0.0.0 only when using **IKE** key management and not **Manual** key management.

### 18.5 VPN Setup Screen

The following figure helps explain the main fields in the web configurator.

**Figure 157** IPSec Summary Fields



Local and remote IP addresses must be static.

Click **Security and VPN** to open the **VPN Setup** screen. This is a menu of your IPSec rules (tunnels). The IPSec summary menu is read-only. Edit a VPN by selecting an index number and then configuring its associated submenus.

**Figure 158** VPN Setup

Summary								
No.	Active	Name:	Local Address	Remote Address	Encap.	IPSec Algorithm	Secure Gateway IP	Modify
1	-	-	...	...	-	-	...	
2	-	-	...	...	-	-	...	
3	-	-	...	...	-	-	...	
4	-	-	...	...	-	-	...	
5	-	-	...	...	-	-	...	
6	-	-	...	...	-	-	...	
7	-	-	...	...	-	-	...	
8	-	-	...	...	-	-	...	
9	-	-	...	...	-	-	...	
10	-	-	...	...	-	-	...	
11	-	-	...	...	-	-	...	
12	-	-	...	...	-	-	...	
13	-	-	...	...	-	-	...	
14	-	-	...	...	-	-	...	
15	-	-	...	...	-	-	...	
16	-	-	...	...	-	-	...	
17	-	-	...	...	-	-	...	
18	-	-	...	...	-	-	...	
19	-	-	...	...	-	-	...	
20	-	-	...	...	-	-	...	

The following table describes the fields in this screen.

**Table 103** VPN Setup

LABEL	DESCRIPTION
No.	This is the VPN policy index number. Click a number to edit VPN policies.
Active	This field displays whether the VPN policy is active or not. A <b>Yes</b> signifies that this VPN policy is active. <b>No</b> signifies that this VPN policy is not active.
Name	This field displays the identification name for this VPN policy.
Local Address	This is the IP address(es) of computer(s) on your local network behind your ZyXEL Device. The same (static) IP address is displayed twice when the <b>Local Address Type</b> field in the <b>VPN-IKE</b> (or <b>VPN-Manual Key</b> ) screen is configured to <b>Single</b> . The beginning and ending (static) IP addresses, in a range of computers are displayed when the <b>Local Address Type</b> field in the <b>VPN-IKE</b> (or <b>VPN-Manual Key</b> ) screen is configured to <b>Range</b> . A (static) IP address and a subnet mask are displayed when the <b>Local Address Type</b> field in the <b>VPN-IKE</b> (or <b>VPN-Manual Key</b> ) screen is configured to <b>Subnet</b> .

**Table 103** VPN Setup

LABEL	DESCRIPTION
Remote Address	This is the IP address(es) of computer(s) on the remote network behind the remote IPSec router. This field displays <b>N/A</b> when the <b>Secure Gateway Address</b> field displays <b>0.0.0.0</b> . In this case only the remote IPSec router can initiate the VPN. The same (static) IP address is displayed twice when the <b>Remote Address Type</b> field in the <b>VPN-IKE</b> (or <b>VPN-Manual Key</b> ) screen is configured to <b>Single</b> . The beginning and ending (static) IP addresses, in a range of computers are displayed when the <b>Remote Address Type</b> field in the <b>VPN-IKE</b> (or <b>VPN-Manual Key</b> ) screen is configured to <b>Range</b> . A (static) IP address and a subnet mask are displayed when the <b>Remote Address Type</b> field in the <b>VPN-IKE</b> (or <b>VPN-Manual Key</b> ) screen is configured to <b>Subnet</b> .
Encap.	This field displays <b>Tunnel</b> or <b>Transport</b> mode ( <b>Tunnel</b> is the default selection).
IPSec Algorithm	This field displays the security protocols used for an SA. Both <b>AH</b> and <b>ESP</b> increase ZyXEL Device processing requirements and communications latency (delay).
Secure Gateway IP	This is the static WAN IP address or URL of the remote IPSec router. This field displays <b>0.0.0.0</b> when you configure the <b>Secure Gateway Address</b> field in the <b>VPN-IKE</b> screen to <b>0.0.0.0</b> .
Modify	Click the <b>Edit</b> icon to go to the screen where you can edit the VPN configuration. Click the <b>Remove</b> icon to remove an existing VPN configuration.
Apply	Click this to save your changes and apply them to the ZyXEL Device.
Cancel	Click this return your settings to their last saved values.

## 18.6 Keep Alive

When you initiate an IPSec tunnel with keep alive enabled, the ZyXEL Device automatically renegotiates the tunnel when the IPSec SA lifetime period expires (see [Section 18.12 on page 288](#) for more on the IPSec SA lifetime). In effect, the IPSec tunnel becomes an “always on” connection after you initiate it. Both IPSec routers must have a ZyXEL Device-compatible keep alive feature enabled in order for this feature to work.

If the ZyXEL Device has its maximum number of simultaneous IPSec tunnels connected to it and they all have keep alive enabled, then no other tunnels can take a turn connecting to the ZyXEL Device because the ZyXEL Device never drops the tunnels that are already connected.

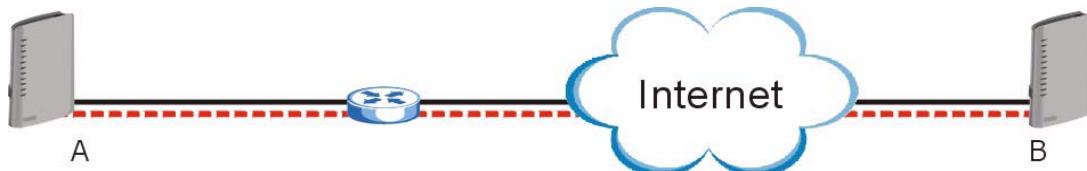
When there is outbound traffic with no inbound traffic, the ZyXEL Device automatically drops the tunnel after two minutes.

## 18.7 VPN, NAT, and NAT Traversal

NAT is incompatible with the AH protocol in both transport and tunnel mode. An IPSec VPN using the AH protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet, but a NAT device between the IPSec endpoints rewrites the source or destination address. As a result, the VPN device at the receiving end finds a mismatch between the hash value and the data and assumes that the data has been maliciously altered.

NAT is not normally compatible with ESP in transport mode either, but the ZyXEL Device's **NAT Traversal** feature provides a way to handle this. NAT traversal allows you to set up an IKE SA when there are NAT routers between the two IPSec routers.

**Figure 159** NAT Router Between IPSec Routers



Normally you cannot set up an IKE SA with a NAT router between the two IPSec routers because the NAT router changes the header of the IPSec packet. NAT traversal solves the problem by adding a UDP port 500 header to the IPSec packet. The NAT router forwards the IPSec packet with the UDP port 500 header unchanged. In [Figure 159 on page 280](#), when IPSec router A tries to establish an IKE SA, IPSec router B checks the UDP port 500 header, and IPSec routers A and B build the IKE SA.

For NAT traversal to work, you must:

- Use ESP security protocol (in either transport or tunnel mode).
- Use IKE keying mode.
- Enable NAT traversal on both IPSec endpoints.
- Set the NAT router to forward UDP port 500 to IPSec router A.

Finally, NAT is compatible with ESP in tunnel mode because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. The compatibility of AH and ESP with NAT in tunnel and transport modes is summarized in the following table.

**Table 104** VPN and NAT

SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	Y*
ESP	Tunnel	Y

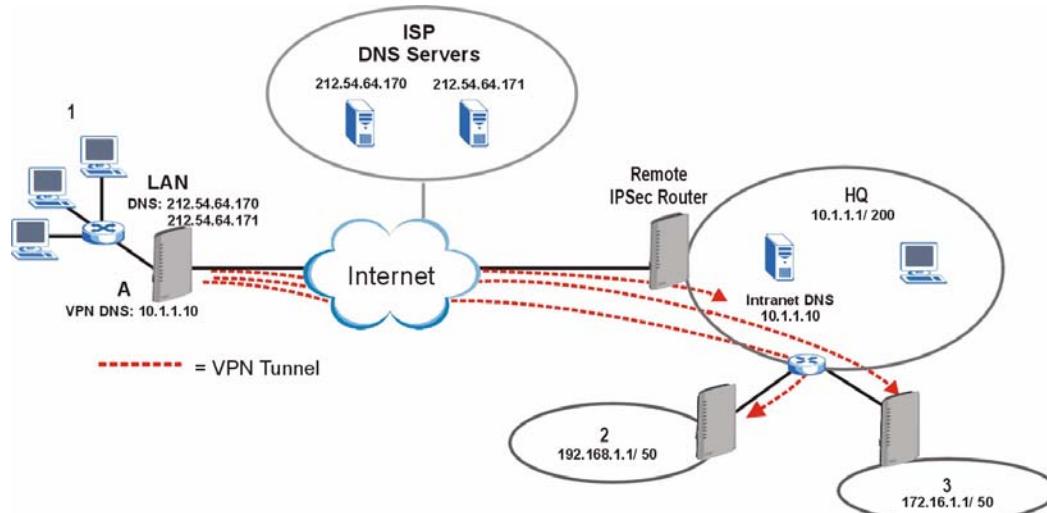
Y\* - This is supported in the ZyXEL Device if you enable NAT traversal.

## 18.8 Remote DNS Server

In cases where you want to use domain names to access Intranet servers on a remote network that has a DNS server, you must identify that DNS server. You cannot use DNS servers on the LAN or from the ISP since these DNS servers cannot resolve domain names to private IP addresses on the remote network.

The following figure depicts an example where three VPN tunnels are created from ZyXEL Device A; one to branch office 2, one to branch office 3 and another to headquarters. In order to access computers that use private domain names on the headquarters (HQ) network, the ZyXEL Device at branch office 1 uses the Intranet DNS server in headquarters. The DNS server feature for VPN does not work with Windows 2000 or Windows XP.

**Figure 160** VPN Host using Intranet DNS Server Example



If you do not specify an Intranet DNS server on the remote network, then the VPN host must use IP addresses to access the computers on the remote network.

## 18.9 ID Type and Content

With aggressive negotiation mode (see[Section 18.12.1 on page 289](#)), the ZyXEL Device identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the ZyXEL Device to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. Telecommuters can use separate passwords to simultaneously connect to the ZyXEL Device from IPSec routers with dynamic IP addresses (see[Section 18.18 on page 297](#) for a telecommuter configuration example).

Regardless of the ID type and content configuration, the ZyXEL Device does not allow you to save multiple active rules with overlapping local and remote IP addresses.

With main mode (see[Section 18.12.1 on page 289](#)), the ID type and content are encrypted to provide identity protection. In this case the ZyXEL Device can only distinguish between up to 12 different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The ZyXEL Device can distinguish up to 12 incoming SAs because you can select between three encryption algorithms (DES, 3DES and AES), two authentication algorithms (MD5 and SHA1) and two key groups (DH1 and DH2) when you configure a VPN rule (see[Section 18.13 on page 289](#)). The ID type and content act as an extra level of identification for incoming SAs.

The type of ID can be a domain name, an IP address or an e-mail address. The content is the IP address, domain name, or e-mail address.

**Table 105** Local ID Type and Content Fields

LOCAL ID TYPE=	CONTENT=
IP	Type the IP address of your computer or leave the field blank to have the ZyXEL Device automatically use its own IP address.
DNS	Type a domain name (up to 31 characters) by which to identify this ZyXEL Device.
E-mail	Type an e-mail address (up to 31 characters) by which to identify this ZyXEL Device.
	The domain name or e-mail address that you use in the <b>Content</b> field is used for identification purposes only and does not need to be a real domain name or e-mail address.

**Table 106** Peer ID Type and Content Fields

PEER ID TYPE=	CONTENT=
IP	Type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the ZyXEL Device automatically use the address in the <b>Secure Gateway</b> field.
DNS	Type a domain name (up to 31 characters) by which to identify the remote IPSec router.
E-mail	Type an e-mail address (up to 31 characters) by which to identify the remote IPSec router.
	The domain name or e-mail address that you use in the <b>Content</b> field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote router's IP address or what you configure in the <b>Secure Gateway Addr</b> field below.

### 18.9.1 ID Type and Content Examples

Two IPSec routers must have matching ID type and content configuration in order to set up a VPN tunnel.

The two ZyXEL Devices in this example can complete negotiation and establish a VPN tunnel.

**Table 107** Matching ID Type and Content Configuration Example

ZYXEL DEVICE A	ZYXEL DEVICE B
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

The two ZyXEL Devices in this example cannot complete their negotiation because ZyXEL Device B's **Local ID type** is **IP**, but ZyXEL Device A's **Peer ID type** is set to **E-mail**. An "ID mismatched" message displays in the IPSEC LOG.

**Table 108** Mismatching ID Type and Content Configuration Example

ZYXEL DEVICE A	ZYXEL DEVICE B
Local ID type: IP	Local ID type: IP
Local ID content: 1.1.1.10	Local ID content: 1.1.1.10
Peer ID type: E-mail	Peer ID type: IP
Peer ID content: aa@yahoo.com	Peer ID content: N/A

## 18.10 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see [Section 18.12 on page 288](#) for more on IKE phases). It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.

## 18.11 Editing VPN Policies

Click an **Edit** icon in the [VPN Setup Screen](#) to edit VPN policies.

**Figure 161** Edit VPN Policies

**IPSec Setup**

- Active
- Keep Alive
- NAT Traversal
- Name:
- IPSec Key Mode:
- Negotiation Mode:
- Encapsulation Mode:
- DNS Server (for IPSec VPN):

**Local**

- Local Address Type:
- IP Address Start:
- End / Subnet Mask:

**Remote**

- Remote Address Type:
- IP Address Start:
- End / Subnet Mask:

**Address Information**

- Local ID Type:
- Content:
- My IP Address:
- Peer ID Type:
- Content:
- Secure Gateway Address:

**Security Protocol**

- VPN Protocol:
- Pre-Shared Key
- Certificate
- Encryption Algorithm:
- Authentication Algorithm:
- auto\_generated\_self\_signed\_cert  (See [My Certificates](#))

**Buttons:** Back, Apply, Cancel, Advanced Setup

The following table describes the fields in this screen.

**Table 109** Edit VPN Policies

LABEL	DESCRIPTION
IPSec Setup	
Active	Select this check box to activate this VPN policy. This option determines whether a VPN rule is applied before a packet leaves the firewall.
Keep Alive	Select either <b>Yes</b> or <b>No</b> from the drop-down list box. Select <b>Yes</b> to have the ZyXEL Device automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The remote IPSec router must also have keep alive enabled in order for this feature to work.
NAT Traversal	This function is available if the <b>VPN protocol</b> is <b>ESP</b> . Select this check box if you want to set up a VPN tunnel when there are NAT routers between the ZyXEL Device and remote IPSec router. The remote IPSec router must also enable NAT traversal, and the NAT routers have to forward UDP port 500 packets to the remote IPSec router behind the NAT router.
Name	Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.

**Table 109** Edit VPN Policies

LABEL	DESCRIPTION
IPSec Key Mode	Select <b>IKE</b> or <b>Manual</b> from the drop-down list box. <b>IKE</b> provides more protection so it is generally recommended. <b>Manual</b> is a useful option for troubleshooting if you have problems using <b>IKE</b> key management.
Negotiation Mode	Select <b>Main</b> or <b>Aggressive</b> from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Encapsulation Mode	Select <b>Tunnel</b> mode or <b>Transport</b> mode from the drop-down list box.
DNS Server (for IPSec VPN)	If there is a private DNS server that services the VPN, type its IP address here. The ZyXEL Device assigns this additional DNS server to the ZyXEL Device's DHCP clients that have IP addresses in this IPSec rule's range of local addresses. A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names.
Local	Specify the IP addresses of the devices behind the ZyXEL Device that can use the VPN tunnel. The local IP addresses must correspond to the remote IPSec router's configured remote IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Local Address Type	Use the drop-down menu to choose <b>Single</b> , <b>Range</b> , or <b>Subnet</b> . Select <b>Single</b> for a single IP address. Select <b>Range</b> for a specific range of IP addresses. Select <b>Subnet</b> to specify IP addresses on a network by their subnet mask.
IP Address Start	When the <b>Local Address Type</b> field is configured to <b>Single</b> , enter a (static) IP address on the LAN behind your ZyXEL Device. When the <b>Local Address Type</b> field is configured to <b>Range</b> , enter the beginning (static) IP address, in a range of computers on your LAN behind your ZyXEL Device. When the <b>Local Address Type</b> field is configured to <b>Subnet</b> , this is a (static) IP address on the LAN behind your ZyXEL Device.
End / Subnet Mask	When the <b>Local Address Type</b> field is configured to <b>Single</b> , this field is N/A. When the <b>Local Address Type</b> field is configured to <b>Range</b> , enter the end (static) IP address, in a range of computers on the LAN behind your ZyXEL Device. When the <b>Local Address Type</b> field is configured to <b>Subnet</b> , this is a subnet mask on the LAN behind your ZyXEL Device.
Remote	Specify the IP addresses of the devices behind the remote IPSec router that can use the VPN tunnel. The remote IP addresses must correspond to the remote IPSec router's configured local IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Remote Address Type	Use the drop-down menu to choose <b>Single</b> , <b>Range</b> , or <b>Subnet</b> . Select <b>Single</b> with a single IP address. Select <b>Range</b> for a specific range of IP addresses. Select <b>Subnet</b> to specify IP addresses on a network by their subnet mask.
IP Address Start	When the <b>Remote Address Type</b> field is configured to <b>Single</b> , enter a (static) IP address on the network behind the remote IPSec router. When the <b>Remote Address Type</b> field is configured to <b>Range</b> , enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the <b>Remote Address Type</b> field is configured to <b>Subnet</b> , enter a (static) IP address on the network behind the remote IPSec router.

**Table 109** Edit VPN Policies

LABEL	DESCRIPTION
End / Subnet Mask	When the <b>Remote Address Type</b> field is configured to <b>Single</b> , this field is N/A. When the <b>Remote Address Type</b> field is configured to <b>Range</b> , enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the <b>Remote Address Type</b> field is configured to <b>Subnet</b> , enter a subnet mask on the network behind the remote IPSec router.
Address Information	
Local ID Type	Select <b>IP</b> to identify this ZyXEL Device by its IP address. Select <b>DNS</b> to identify this ZyXEL Device by a domain name. Select <b>E-mail</b> to identify this ZyXEL Device by an e-mail address.
Content	When you select <b>IP</b> in the <b>Local ID Type</b> field, type the IP address of your computer in the local <b>Content</b> field. The ZyXEL Device automatically uses the IP address in the <b>My IP Address</b> field (refer to the <b>My IP Address</b> field description) if you configure the local <b>Content</b> field to <b>0.0.0.0</b> or leave it blank. It is recommended that you type an IP address other than <b>0.0.0.0</b> in the local <b>Content</b> field or use the <b>DNS</b> or <b>E-mail</b> ID type in the following situations. When there is a NAT router between the two IPSec routers. When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses. When you select <b>DNS</b> or <b>E-mail</b> in the <b>Local ID Type</b> field, type a domain name or e-mail address by which to identify this ZyXEL Device in the local <b>Content</b> field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.
My IP Address	Enter the WAN IP address of your ZyXEL Device. The VPN tunnel has to be rebuilt if this IP address changes. The following applies if this field is configured as <b>0.0.0.0</b> : The ZyXEL Device uses the current ZyXEL Device WAN IP address (static or dynamic) to set up the VPN tunnel. If the WAN connection goes down, the ZyXEL Device uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See <a href="#">Chapter 7 on page 101</a> for details on dial backup and traffic redirect.
Peer ID Type	Select <b>IP</b> to identify the remote IPSec router by its IP address. Select <b>DNS</b> to identify the remote IPSec router by a domain name. Select <b>E-mail</b> to identify the remote IPSec router by an e-mail address.
Content	The configuration of the peer content depends on the peer ID type. For <b>IP</b> , type the IP address of the computer with which you will make the VPN connection. If you configure this field to <b>0.0.0.0</b> or leave it blank, the ZyXEL Device will use the address in the <b>Secure Gateway Address</b> field (refer to the <b>Secure Gateway Address</b> field description). For <b>DNS</b> or <b>E-mail</b> , type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string. It is recommended that you type an IP address other than <b>0.0.0.0</b> or use the <b>DNS</b> or <b>E-mail</b> ID type in the following situations: When there is a NAT router between the two IPSec routers. When you want the ZyXEL Device to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses.

**Table 109** Edit VPN Policies

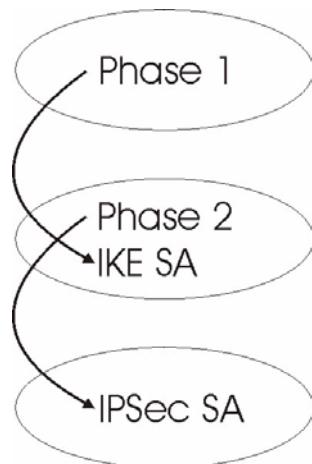
LABEL	DESCRIPTION
Secure Gateway Address	Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to <b>0.0.0.0</b> if the remote IPSec router has a dynamic WAN IP address (the <b>Key Management</b> field must be set to <b>IKE</b> ). In order to have more than one active rule with the <b>Secure Gateway Address</b> field set to <b>0.0.0.0</b> , the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with <b>0.0.0.0</b> in the <b>Secure Gateway Address</b> field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the <b>Secure Gateway Address</b> field set to <b>0.0.0.0</b> .
Security Protocol	
VPN Protocol	Select <b>ESP</b> if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by <b>AH</b> . If you select <b>ESP</b> here, you must select options from the <b>Encryption Algorithm</b> and <b>Authentication Algorithm</b> fields (described below).
Pre-Shared Key	Click the button to use a pre-shared key for authentication, and type in your pre-shared key. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", "0x" denotes that the key is hexadecimal and "0123456789ABCDEF" is the key itself. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a "PYLD_MALFORMED" (payload malformed) packet if the same pre-shared key is not used on both ends.
Certificate	Click the button to use a certificate for authentication. Select the certificate you want to use from the list. You can create, import and configure certificates in the <b>Security &gt; Certificates</b> screens, or click the <b>My Certificates</b> link.
My Certificates	Click this to go to the <b>Security &gt; Certificates &gt; My Certificates</b> screen. If you do not click <b>Apply</b> first, your VPN settings will not be saved.
Encryption Algorithm	Select <b>DES</b> , <b>3DES</b> , <b>AES</b> or <b>NULL</b> from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The <b>DES</b> encryption algorithm uses a 56-bit key. <b>Triple DES (3DES)</b> is a variation on <b>DES</b> that uses a 168-bit key. As a result, <b>3DES</b> is more secure than <b>DES</b> . It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of <b>AES</b> uses a 128-bit key. <b>AES</b> is faster than <b>3DES</b> . Select <b>NULL</b> to set up a tunnel without encryption. When you select <b>NULL</b> , you do not enter an encryption key.
Authentication Algorithm	Select <b>SHA1</b> or <b>MD5</b> from the drop-down list box. <b>MD5</b> (Message Digest 5) and <b>SHA1</b> (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The <b>SHA1</b> algorithm is generally considered stronger than <b>MD5</b> , but is slower. Select <b>MD5</b> for minimal security and <b>SHA-1</b> for maximum security.
Advanced Setup	Click <b>Advanced</b> to configure more detailed settings of your IKE key management.
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.

**Table 109** Edit VPN Policies

LABEL	DESCRIPTION
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Advanced Setup	Click <b>Advanced Setup</b> to configure more detailed settings of your IKE key management.

## 18.12 IKE Phases

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

**Figure 162** Two Phases to Set Up the IPSec SA

In phase 1 you must:

- Choose a negotiation mode.
- Authenticate the connection by entering a pre-shared key.
- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose a Diffie-Hellman public-key cryptography key group (**DH1** or **DH2**).
- Set the IKE SA lifetime. This field allows you to determine how long an IKE SA should stay up before it times out. An IKE SA times out when the IKE SA lifetime period expires. If an IKE SA times out when an IPSec SA is already established, the IPSec SA stays connected.

In phase 2 you must:

- Choose which protocol to use (**ESP** or **AH**) for the IKE key exchange.
- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose whether to enable Perfect Forward Secrecy (PFS) using Diffie-Hellman public-key cryptography – see [Section 18.12.3 on page 289](#). Select **None** (the default) to disable PFS.
- Choose **Tunnel** mode or **Transport** mode.

- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The ZyXEL Device automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. The ZyXEL Device also automatically renegotiates the IPSec SA if both IPSec routers have keep alive enabled, even if there is no traffic. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

### 18.12.1 Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

- **Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips: SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).
- **Aggressive Mode** is quicker than **Main Mode** because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not known by the responder and both parties want to use pre-shared key authentication.

### 18.12.2 Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. 768-bit (Group 1 - **DH1**) and 1024-bit (Group 2 - **DH2**) Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

### 18.12.3 Perfect Forward Secrecy (PFS)

Enabling PFS means that the key is transient. The key is thrown away and replaced by a brand new key using a new Diffie-Hellman exchange for each new IPSec SA setup. With PFS enabled, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys. The (time-consuming) Diffie-Hellman exchange is the trade-off for this extra security.

This may be unnecessary for data that does not require such security, so PFS is disabled (**None**) by default in the ZyXEL Device. Disabling PFS means new authentication and encryption keys are derived from the same root secret (which may have security implications in the long run) but allows faster SA setup (by bypassing the Diffie-Hellman key exchange).

## 18.13 Configuring Advanced IKE Settings

Click **Advanced Setup** in the [Edit VPN Policies](#) screen to open this screen.

**Figure 163** Advanced VPN Policies

**VPN - IKE - Advanced Setup**

Protocol	0
Enable Replay Detection	NO
Local Start Port	0 End 0
Remote Start Port	0 End 0

**Phase1**

Negotiation Mode	Main
Pre-Shared Key	(empty)
Encryption Algorithm	DES
Authentication Algorithm	MD5
SA Life Time (Seconds)	28800
Key Group	DH1

**Phase2**

Active Protocol	ESP
Encryption Algorithm	DES
Authentication Algorithm	SHA1
SA Life Time (Seconds)	28800
Encapsulation	Tunnel
Perfect Forward Secrecy (PFS)	NONE

Back    Apply    Cancel

The following table describes the fields in this screen.

**Table 110** Advanced VPN Policies

LABEL	DESCRIPTION
VPN - IKE	
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DoS) attacks. The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Select <b>YES</b> from the drop-down menu to enable replay detection, or select <b>NO</b> to disable it.
Local Start Port	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If <b>Local Start Port</b> is left at 0, <b>End</b> will also remain at 0.
Remote Start Port	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If <b>Remote Start Port</b> is left at 0, <b>End</b> will also remain at 0.
Phase 1	
Negotiation Mode	Select <b>Main</b> or <b>Aggressive</b> from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.

**Table 110** Advanced VPN Policies

LABEL	DESCRIPTION
Pre-Shared Key	Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62-character range for the key. For example, in "0x0123456789ABCDEF", "0x" denotes that the key is hexadecimal and "0123456789ABCDEF" is the key itself. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a "PYLD_MALFORMED" (payload malformed) packet if the same pre-shared key is not used on both ends.
Encryption Algorithm	Select <b>DES</b> , <b>3DES</b> or <b>AES</b> from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES ( <b>3DES</b> ) is a variation on <b>DES</b> that uses a 168-bit key. As a result, <b>3DES</b> is more secure than <b>DES</b> . It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of AES uses a 128-bit key. <b>AES</b> is faster than <b>3DES</b> .
Authentication Algorithm	Select <b>SHA1</b> or <b>MD5</b> from the drop-down list box. <b>MD5</b> (Message Digest 5) and <b>SHA1</b> (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The <b>SHA1</b> algorithm is generally considered stronger than <b>MD5</b> , but is slower. Select <b>MD5</b> for minimal security and <b>SHA-1</b> for maximum security.
SA Life Time (Seconds)	Define the length of time before an IPSec SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Key Group	You must choose a key group for phase 1 IKE setup. <b>DH1</b> (default) refers to Diffie-Hellman Group 1 a 768 bit random number. <b>DH2</b> refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.
Phase 2	
Active Protocol	Use the drop-down list box to choose from <b>ESP</b> or <b>AH</b> .
Encryption Algorithm	This field is available when you select <b>ESP</b> in the <b>Active Protocol</b> field. Select <b>DES</b> , <b>3DES</b> , <b>AES</b> or <b>NULL</b> from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES ( <b>3DES</b> ) is a variation on DES that uses a 168-bit key. As a result, <b>3DES</b> is more secure than <b>DES</b> . It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of AES uses a 128-bit key. <b>AES</b> is faster than <b>3DES</b> . Select <b>NULL</b> to set up a tunnel without encryption. When you select <b>NULL</b> , you do not enter an encryption key.
Authentication Algorithm	Select <b>SHA1</b> or <b>MD5</b> from the drop-down list box. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The SHA1 algorithm is generally considered stronger than MD5, but is slower. Select <b>MD5</b> for minimal security and <b>SHA-1</b> for maximum security.

**Table 110** Advanced VPN Policies

LABEL	DESCRIPTION
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Encapsulation	Select <b>Tunnel</b> mode or <b>Transport</b> mode from the drop-down list box.
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled ( <b>NONE</b> ) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Choose <b>DH1</b> or <b>DH2</b> from the drop-down list box to enable PFS. <b>DH1</b> refers to Diffie-Hellman Group 1 a 768 bit random number. <b>DH2</b> refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number (more secure, yet slower).
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device and return to the <b>VPN-IKE</b> screen.
Cancel	Click <b>Cancel</b> to return to the <b>VPN-IKE</b> screen without saving your changes.

## 18.14 Manual Key Setup

Manual key management is useful if you have problems with **IKE** key management.

### 18.14.1 Security Parameter Index (SPI)

An SPI is used to distinguish different SAs terminating at the same destination and using the same IPSec protocol. This data allows for the multiplexing of SAs to a single gateway. The **SPI** (Security Parameter Index) along with a destination IP address uniquely identify a particular Security Association (SA). The **SPI** is transmitted from the remote VPN gateway to the local VPN gateway. The local VPN gateway then uses the network, encryption and key values that the administrator associated with the SPI to establish the tunnel.

Current ZyXEL implementation assumes identical outgoing and incoming SPIs.

## 18.15 Configuring Manual Key

You only configure **VPN Manual Key** when you select **Manual** in the **IPSec Key Mode** field on the **VPN IKE** screen. This is the **VPN Manual Key** screen as shown next.

**Figure 164** VPN: Manual Key

The following table describes the fields in this screen.

**Table 111** VPN: Manual Key

LABEL	DESCRIPTION
IPSec Setup	
Active	Select this check box to activate this VPN policy.
Name	Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
IPSec Key Mode	Select <b>IKE</b> or <b>Manual</b> from the drop-down list box. <b>Manual</b> is a useful option for troubleshooting if you have problems using <b>IKE</b> key management.
SPI	Type a number (base 10) from 1 to 999999 for the Security Parameter Index.
Encapsulation Mode	Select <b>Tunnel</b> mode or <b>Transport</b> mode from the drop-down list box.

**Table 111** VPN: Manual Key (continued)

LABEL	DESCRIPTION
DNS Server (for IPSec VPN)	If there is a private DNS server that services the VPN, type its IP address here. The ZyXEL Device assigns this additional DNS server to the ZyXEL Device's DHCP clients that have IP addresses in this IPSec rule's range of local addresses. A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names.
Local	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Local Address Type	Use the drop-down menu to choose <b>Single</b> , <b>Range</b> , or <b>Subnet</b> . Select <b>Single</b> for a single IP address. Select <b>Range</b> for a specific range of IP addresses. Select <b>Subnet</b> to specify IP addresses on a network by their subnet mask.
IP Address Start	When the <b>Local Address Type</b> field is configured to <b>Single</b> , enter a (static) IP address on the LAN behind your ZyXEL Device. When the <b>Local Address Type</b> field is configured to <b>Range</b> , enter the beginning (static) IP address, in a range of computers on your LAN behind your ZyXEL Device. When the <b>Local Address Type</b> field is configured to <b>Subnet</b> , this is a (static) IP address on the LAN behind your ZyXEL Device.
End / Subnet Mask	When the <b>Local Address Type</b> field is configured to <b>Single</b> , this field is N/A. When the <b>Local Address Type</b> field is configured to <b>Range</b> , enter the end (static) IP address, in a range of computers on the LAN behind your ZyXEL Device. When the <b>Local Address Type</b> field is configured to <b>Subnet</b> , this is a subnet mask on the LAN behind your ZyXEL Device.
Remote	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Remote Address Type	Use the drop-down menu to choose <b>Single</b> , <b>Range</b> , or <b>Subnet</b> . Select <b>Single</b> with a single IP address. Select <b>Range</b> for a specific range of IP addresses. Select <b>Subnet</b> to specify IP addresses on a network by their subnet mask.
IP Address Start	When the <b>Remote Address Type</b> field is configured to <b>Single</b> , enter a (static) IP address on the network behind the remote IPSec router. When the <b>Remote Address Type</b> field is configured to <b>Range</b> , enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the <b>Remote Address Type</b> field is configured to <b>Subnet</b> , enter a (static) IP address on the network behind the remote IPSec router.
End / Subnet Mask	When the <b>Remote Address Type</b> field is configured to <b>Single</b> , this field is N/A. When the <b>Remote Address Type</b> field is configured to <b>Range</b> , enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the <b>Remote Address Type</b> field is configured to <b>Subnet</b> , enter a subnet mask on the network behind the remote IPSec router.
Address Information	

**Table 111** VPN: Manual Key (continued)

LABEL	DESCRIPTION
My IP Address	Enter the WAN IP address of your ZyXEL Device. The VPN tunnel has to be rebuilt if this IP address changes. The following applies if this field is configured as <b>0.0.0.0</b> : The ZyXEL Device uses the current ZyXEL Device WAN IP address (static or dynamic) to set up the VPN tunnel. If the WAN connection goes down, the ZyXEL Device uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See <a href="#">Chapter 7 on page 101</a> for details on dial backup and traffic redirect.
Secure Gateway Address	Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection.
Security Protocol	
IPSec Protocol	Select <b>ESP</b> if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by <b>AH</b> . If you select ESP here, you must select options from the <b>Encryption Algorithm</b> and <b>Authentication Algorithm</b> fields (described next).
Encryption Algorithm	Select <b>DES</b> , <b>3DES</b> or <b>NULL</b> from the drop-down list box. When <b>DES</b> is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The <b>DES</b> encryption algorithm uses a 56-bit key. Triple DES ( <b>3DES</b> ) is a variation on <b>DES</b> that uses a 168-bit key. As a result, <b>3DES</b> is more secure than <b>DES</b> . It also requires more processing power, resulting in increased latency and decreased throughput. Select <b>NULL</b> to set up a tunnel without encryption. When you select <b>NULL</b> , you do not enter an encryption key.
Encapsulation Key (only with ESP)	With <b>DES</b> , type a unique key 8 characters long. With <b>3DES</b> , type a unique key 24 characters long. Any characters may be used, including spaces, but trailing spaces are truncated.
Authentication Algorithm	Select <b>SHA1</b> or <b>MD5</b> from the drop-down list box. <b>MD5</b> (Message Digest 5) and <b>SHA1</b> (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The <b>SHA1</b> algorithm is generally considered stronger than <b>MD5</b> , but is slower. Select <b>MD5</b> for minimal security and <b>SHA-1</b> for maximum security.
Authentication Key	Type a unique authentication key to be used by IPSec if applicable. Enter 16 characters for <b>MD5</b> authentication or 20 characters for <b>SHA-1</b> authentication. Any characters may be used, including spaces, but trailing spaces are truncated.
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.

## 18.16 Viewing SA Monitor

Click **Security**, **VPN** and **Monitor** to open the **SA Monitor** screen as shown. Use this screen to display and manage active VPN connections.

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This screen displays active VPN connections. Use **Refresh** to display active VPN connections. This screen is read-only. The following table describes the fields in this tab.

When there is outbound traffic but no inbound traffic, the SA times out automatically after two minutes. A tunnel with no outbound or inbound traffic is "idle" and does not timeout until the SA lifetime period expires. See [Section 18.6 on page 279](#) on keep alive to have the ZyXEL Device renegotiate an IPSec SA when the SA lifetime expires, even if there is no traffic.

**Figure 165** VPN: SA Monitor

Monitor				
	No.	Name:	Encapsulation	IP Sec Algorithm
<input type="radio"/>	1	-	-	-
<input type="radio"/>	2	-	-	-
<input type="radio"/>	3	-	-	-
<input type="radio"/>	4	-	-	-
<input type="radio"/>	5	-	-	-
<input type="radio"/>	6	-	-	-
<input type="radio"/>	7	-	-	-
<input type="radio"/>	8	-	-	-
<input type="radio"/>	9	-	-	-
<input type="radio"/>	10	-	-	-
<input type="radio"/>	11	-	-	-
<input type="radio"/>	12	-	-	-
<input type="radio"/>	13	-	-	-
<input type="radio"/>	14	-	-	-
<input type="radio"/>	15	-	-	-
<input type="radio"/>	16	-	-	-
<input type="radio"/>	17	-	-	-
<input type="radio"/>	18	-	-	-
<input type="radio"/>	19	-	-	-
<input type="radio"/>	20	-	-	-

The following table describes the fields in this screen.

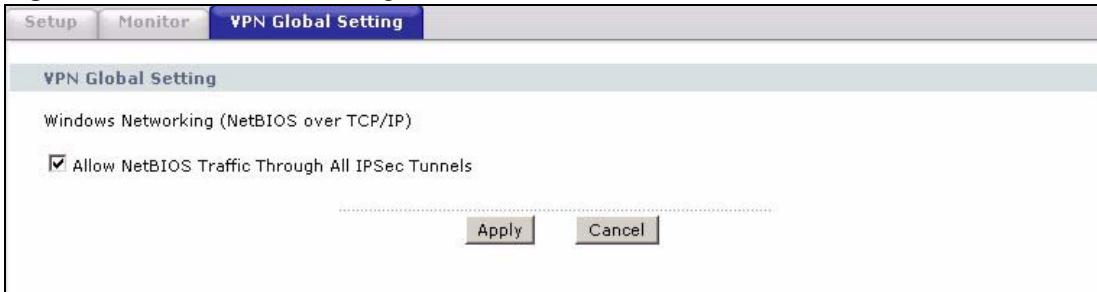
**Table 112** VPN: SA Monitor

LABEL	DESCRIPTION
No	This is the security association index number.
Name	This field displays the identification name for this VPN policy.
Encapsulation	This field displays <b>Tunnel</b> or <b>Transport</b> mode.
IPSec Algorithm	This field displays the security protocol, encryption algorithm, and authentication algorithm used in each VPN tunnel.
Disconnect	Select one of the security associations, and then click <b>Disconnect</b> to stop that security association.
Refresh	Click <b>Refresh</b> to display the current active VPN connection(s).

## 18.17 Configuring Global Setting

To change your ZyXEL Device's global settings, click **VPN** and then **Global Setting**. The screen appears as shown.

**Figure 166** VPN: Global Setting



The following table describes the fields in this screen.

**Table 113** VPN: Global Setting

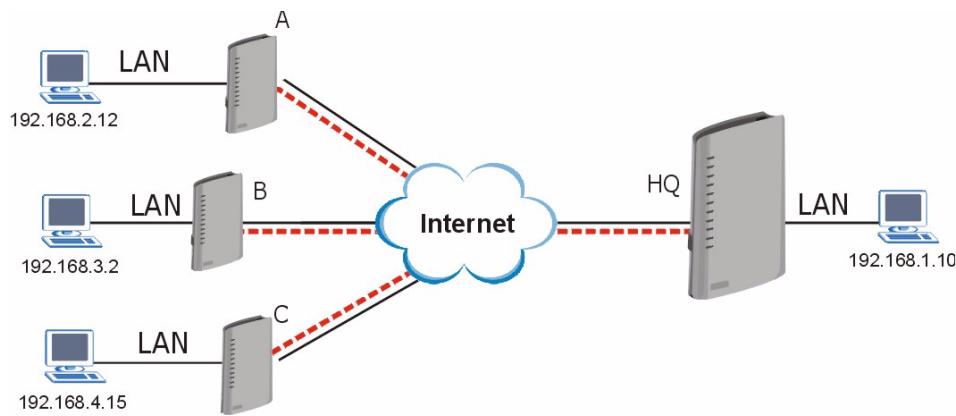
LABEL	DESCRIPTION
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to find other computers. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa.
Allow NetBIOS Traffic Through All IPSec Tunnels	Select this check box to send NetBIOS packets through the VPN connection.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 18.18 Telecommuter VPN/IPSec Examples

The following examples show how multiple telecommuters can make VPN connections to a single ZyXEL Device at headquarters. The telecommuters use IPSec routers with dynamic WAN IP addresses. The ZyXEL Device at headquarters has a static public IP address.

### 18.18.1 Telecommuters Sharing One VPN Rule Example

See the following figure and table for an example configuration that allows multiple telecommuters (A, B and C in the figure) to use one VPN rule to simultaneously access a ZyXEL Device at headquarters (HQ in the figure). The telecommuters do not have domain names mapped to the WAN IP addresses of their IPSec routers. The telecommuters must all use the same IPSec parameters but the local IP addresses (or ranges of addresses) should not overlap.

**Figure 167** Telecommuters Sharing One VPN Rule Example**Table 114** Telecommuters Sharing One VPN Rule Example

FIELDS	TELECOMMUTERS	HEADQUARTERS
My IP Address:	0.0.0.0 (dynamic IP address assigned by the ISP)	Public static IP address
Secure Gateway IP Address:	Public static IP address	0.0.0.0 With this IP address only the telecommuter can initiate the IPSec tunnel.
Local IP Address:	Telecommuter A: 192.168.2.12 Telecommuter B: 192.168.3.2 Telecommuter C: 192.168.4.15	192.168.1.10
Remote IP Address:	192.168.1.10	0.0.0.0 (N/A)

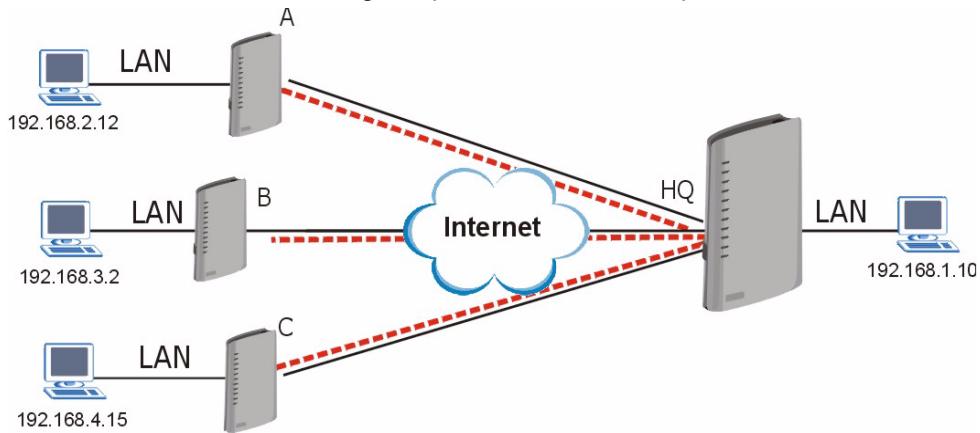
### 18.18.2 Telecommuters Using Unique VPN Rules Example

In this example the telecommuters (A, B and C in the figure) use IPSec routers with domain names that are mapped to their dynamic WAN IP addresses (use Dynamic DNS to do this).

With aggressive negotiation mode (see [Section 18.12.1 on page 289](#)), the ZyXEL Device can use the ID types and contents to distinguish between VPN rules. Telecommuters can each use a separate VPN rule to simultaneously access a ZyXEL Device at headquarters. They can use different IPSec parameters. The local IP addresses (or ranges of addresses) of the rules configured on the ZyXEL Device at headquarters can overlap. The local IP addresses of the rules configured on the telecommuters' IPSec routers should not overlap.

See the following table and figure for an example where three telecommuters each use a different VPN rule for a VPN connection with a ZyXEL Device located at headquarters. The ZyXEL Device at headquarters (HQ in the figure) identifies each incoming SA by its ID type and content and uses the appropriate VPN rule to establish the VPN connection.

The ZyXEL Device at headquarters can also initiate VPN connections to the telecommuters since it can find the telecommuters by resolving their domain names.

**Figure 168** Telecommuters Using Unique VPN Rules Example**Table 115** Telecommuters Using Unique VPN Rules Example

TELECOMMUTERS	HEADQUARTERS
All Telecommuter Rules:	All Headquarters Rules:
My IP Address 0.0.0.0	My IP Address: bigcompanyhq.com
Secure Gateway Address: bigcompanyhq.com	Local IP Address: 192.168.1.10
Remote IP Address: 192.168.1.10	Local ID Type: E-mail
Peer ID Type: E-mail	Local ID Content: bob@bigcompanyhq.com
Peer ID Content: bob@bigcompanyhq.com	
Telecommuter A (telecommutera.dydns.org)	Headquarters ZyXEL Device Rule 1:
Local ID Type: IP	Peer ID Type: IP
Local ID Content: 192.168.2.12	Peer ID Content: 192.168.2.12
Local IP Address: 192.168.2.12	Secure Gateway Address: telecommuter1.com
	Remote Address 192.168.2.12
Telecommuter B (telecommuterb.dydns.org)	Headquarters ZyXEL Device Rule 2:
Local ID Type: DNS	Peer ID Type: DNS
Local ID Content: telecommuterb.com	Peer ID Content: telecommuterb.com
Local IP Address: 192.168.3.2	Secure Gateway Address: telecommuterb.com
	Remote Address 192.168.3.2
Telecommuter C (telecommuterc.dydns.org)	Headquarters ZyXEL Device Rule 3:
Local ID Type: E-mail	Peer ID Type: E-mail
Local ID Content: myVPN@myplace.com	Peer ID Content: myVPN@myplace.com
Local IP Address: 192.168.4.15	Secure Gateway Address: telecommuterc.com
	Remote Address 192.168.4.15

## 18.19 VPN and Remote Management

If a VPN tunnel uses Telnet, FTP, WWW, then you should configure remote management (**Remote Management**) to allow access for that service.

# Certificates

This chapter gives background information about public-key certificates and explains how to use them.

## 19.1 Certificates Overview

The ZyXEL Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the ZyXEL Device to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

- 1 Tim wants to send a private message to Jenny. Tim generates a public key pair. What is encrypted with one key can only be decrypted using the other.
- 2 Tim keeps the private key and makes the public key openly available.
- 3 Tim uses his private key to encrypt the message and sends it to Jenny.
- 4 Jenny receives the message and uses Tim's public key to decrypt it.
- 5 Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The ZyXEL Device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The ZyXEL Device does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The ZyXEL Device can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (Public-Key Infrastructure).

### 19.1.1 Advantages of Certificates

Certificates offer the following benefits.

- The ZyXEL Device only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

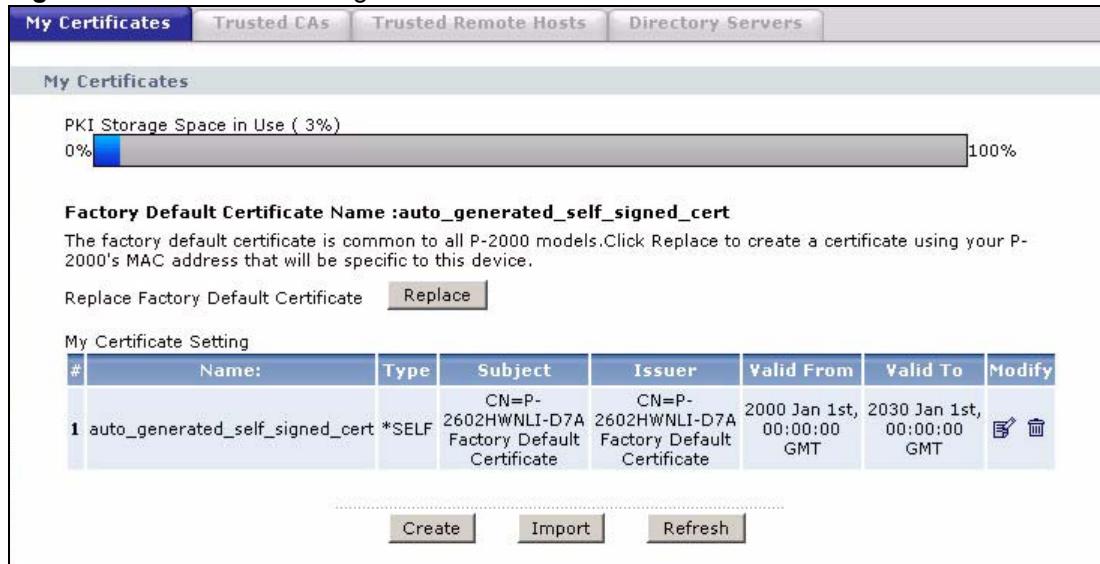
## 19.2 Self-signed Certificates

You can have the ZyXEL Device act as a certification authority and sign its own certificates.

## 19.3 Configuration Summary

This section summarizes how to manage certificates on the ZyXEL Device.

**Figure 169** Certificate Configuration Overview



Use the **My Certificates** screens to generate and export self-signed certificates or certification requests and import the ZyXEL Device's CA-signed certificates.

Use the **Trusted CAs** screens to save CA certificates to the ZyXEL Device.

Use the **Trusted Remote Hosts** screens to import self-signed certificates.

Use the **Directory Servers** screen to configure a list of addresses of directory servers (that contain lists of valid and revoked certificates).

## 19.4 My Certificates

Click **Security > Certificates > My Certificates** to open the **My Certificates** screen. This is the ZyXEL Device's summary list of certificates and certification requests. Certificates display in black and certification requests display in gray.

**Figure 170** My Certificates



The following table describes the labels in this screen.

**Table 116** My Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyXEL Device's PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
Replace	This button displays when the ZyXEL Device has the factory default certificate. The factory default certificate is common to all ZyXEL Devices that use certificates. ZyXEL recommends that you use this button to replace the factory default certificate with one that uses your ZyXEL Device's MAC address.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Type	This field displays what kind of certificate this is. <b>REQ</b> represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the <b>My Certificate Import</b> screen to import the certificate and replace the request. <b>SELF</b> represents a self-signed certificate. <b>*SELF</b> represents the default self-signed certificate, which the ZyXEL Device uses to sign imported trusted remote host certificates. <b>CERT</b> represents a certificate issued by a certification authority.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.

**Table 116** My Certificates (continued)

LABEL	DESCRIPTION
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the <b>Subject</b> field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Modify	<p>Click the details icon to open a screen with an in-depth list of information about the certificate.</p> <p>Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate.</p> <p>You cannot delete a certificate that one or more features is configured to use.</p> <p>Do the following to delete a certificate that shows *SELF in the <b>Type</b> field.</p> <ol style="list-style-type: none"> <li>1. Make sure that no other features, such as HTTPS, VPN, SSH are configured to use the *SELF certificate.</li> <li>2. Click the details icon next to another self-signed certificate (see the description on the <b>Create</b> button if you need to create a self-signed certificate).</li> <li>3. Select the <b>Default self-signed certificate which signs the imported remote host certificates</b> check box.</li> <li>4. Click <b>Apply</b> to save the changes and return to the <b>My Certificates</b> screen.</li> <li>5. The certificate that originally showed *SELF displays SELF and you can delete it now.</li> </ol> <p>Note that subsequent certificates move up by one when you take this action</p>
Create	Click <b>Create</b> to go to the screen where you can have the ZyXEL Device generate a certificate or a certification request.
Import	Click <b>Import</b> to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the ZyXEL Device.
Refresh	Click <b>Refresh</b> to display the current validity status of the certificates.

## 19.5 My Certificate Import

Click **Security > Certificates > My Certificates** and then **Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate to the ZyXEL Device.



You can only import a certificate that matches a corresponding certification request that was generated by the ZyXEL Device.



The certificate you import replaces the corresponding request in the **My Certificates** screen.



You must remove any spaces from the certificate's filename before you can import it.

### 19.5.1 Certificate File Formats

The certification authority certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. The ZyXEL Device currently allows the importation of a PKCS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses 64 ASCII characters to convert a binary PKCS#7 certificate into a printable form.

**Figure 171** My Certificate Import

Certificates - MY Certificates - Import

Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7

For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on Prestige. After the importation, the certification request will automatically be deleted.

File Path:

The following table describes the labels in this screen.

**Table 117** My Certificate Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse</b> to find it.
Browse	Click <b>Browse</b> to find the certificate file you want to upload.
Back	Click <b>Back</b> to return to the previous screen.

**Table 117** My Certificate Import

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save the certificate on the ZyXEL Device.
Cancel	Click <b>Cancel</b> to clear your settings.

## 19.6 My Certificate Create

Click **Security > Certificates > My Certificates > Create** to open the **My Certificate Create** screen. Use this screen to have the ZyXEL Device create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request.

**Figure 172** My Certificate Create

The following table describes the labels in this screen.

**Table 118** My Certificate Create

LABEL	DESCRIPTION
Certificate Name	Type up to 31 ASCII characters (not including spaces) to identify this certificate.
Subject Information	Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although the <b>Common Name</b> is mandatory. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information.
Common Name	Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.

**Table 118** My Certificate Create (continued)

LABEL	DESCRIPTION
Organizational Unit	Type up to 127 characters to identify the organizational unit or department to which the certificate owner belongs. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
Organization	Type up to 127 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
Country	Type up to 127 characters to identify the nation where the certificate owner is located. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Enrollment Options	These radio buttons deal with how and when the certificate is to be generated.
Create a self-signed certificate	Select <b>Create a self-signed certificate</b> to have the ZyXEL Device generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.
Create a certification request and save it locally for later manual enrollment	Select <b>Create a certification request and save it locally for later manual enrollment</b> to have the ZyXEL Device generate and store a request for a certificate. Use the <b>My Certificate Details</b> screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the <b>My Certificate Details</b> screen (see <a href="#">Section 19.7 on page 308</a> ) and then send it to the certification authority.
Create a certification request and enroll for a certificate immediately online	Select <b>Create a certification request and enroll for a certificate immediately online</b> to have the ZyXEL Device generate a request for a certificate and apply to a certification authority for a certificate. You must have the certification authority's certificate already imported in the <b>Trusted CAs</b> screen. When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the <b>Reference Number</b> and <b>Key</b> if the certification authority requires them.
Enrollment Protocol	Select the certification authority's enrollment protocol from the drop-down list box. <b>Simple Certificate Enrollment Protocol (SCEP)</b> is a TCP-based enrollment protocol that was developed by VeriSign and Cisco. <b>Certificate Management Protocol (CMP)</b> is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510.
CA Server Address	Enter the IP address (or URL) of the certification authority server.
CA Certificate	Select the certification authority's certificate from the <b>CA Certificate</b> drop-down list box. You must have the certification authority's certificate already imported in the <b>Trusted CAs</b> screen. Click <b>Trusted CAs</b> to go to the <b>Trusted CAs</b> screen where you can view (and manage) the ZyXEL Device's list of certificates of trusted certification authorities.
Request Authentication	When you select <b>Create a certification request and enroll for a certificate immediately online</b> , the certification authority may want you to include a reference number and key to identify you when you send a certification request. Fill in both the <b>Reference Number</b> and the <b>Key</b> fields if your certification authority uses CMP enrollment protocol. Just fill in the <b>Key</b> field if your certification authority uses the SCEP enrollment protocol.

**Table 118** My Certificate Create (continued)

LABEL	DESCRIPTION
Key	Type the key that the certification authority gave you.
Apply	Click <b>Apply</b> to begin certificate or certification request generation.
Cancel	Click <b>Cancel</b> to quit and return to the <b>My Certificates</b> screen.

After you click **Apply** in the **My Certificate Create** screen, you see a screen that tells you the ZyXEL Device is generating the self-signed certificate or certification request.

After the ZyXEL Device successfully enrolls a certificate or generates a certification request or a self-signed certificate, you see a screen with a **Return** button that takes you back to the **My Certificates** screen.

If you configured the **My Certificate Create** screen to have the ZyXEL Device enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **My Certificate Create** screen. Click **Return** and check your information in the **My Certificate Create** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the ZyXEL Device to enroll a certificate online.

## 19.7 My Certificate Details

Click **Security > Certificates > My Certificates** to open the **My Certificates** screen (see [Figure 170 on page 303](#)). Click the edit icon to open the **My Certificate Details** screen. Use this screen to view in-depth certificate information and change the certificate's name. In the case of a self-signed certificate, you can set it to be the one that the ZyXEL Device uses to sign the trusted remote host certificates that you import to the ZyXEL Device.

**Figure 173** My Certificate Details

**Certificates - My Certificates - Details**

<b>Certificate Name</b>	auto_generated_self_signed_cert
<b>Property</b>	
<input checked="" type="checkbox"/> Default self-signed certificate which signs the imported remote host certificates.	
<b>Certificate Path</b>	
<div style="border: 1px solid #ccc; padding: 5px; height: 100px;">           Searching...           <div style="text-align: right; margin-top: 5px;"> <input type="button" value="Refresh"/> </div> </div>	
<b>Certificate Informations</b>	
Type	Self-signed X.509 Certificate
Version	V3
Serial Number	947027954
Subject	CN=P2-D1 001349000001
Issuer	CN=P2-D1 001349000001
Signature Algorithm	rsa-pkcs1-sha1
Valid From	2000 Jan 1st, 00:00:00 GMT
Valid To	2030 Jan 1st, 00:00:00 GMT
Key Algorithm	rsaEncryption (512 bits)
Subject Alternative Name	EMAIL=001349000001@auto.gen.cert
Key Usage	DigitalSignature, KeyEncipherment, KeyCertSign
Basic Constraint	Subject Type=CA, Path Length Constraint=1
MD5 Fingerprint	1d:a8:68:8e:f2:5d:8f:a7:03:65:e0:b2:af:13:e9:a7
SHA1 Fingerprint	e4:97:2a:ca:8b:c5:09:59:84:51:db:bd:f6:4e:4d:eb:6e:9c:d0:fa

**Certificate in PEM (Base-64) Encoded Format**

```
-----BEGIN CERTIFICATE-----
MIIBhTCCAS+gAwIBAgIEOG1M/zANBgkqhkiG9wOBAQUFADAiMSAwHgYDVQQDExdQ
NjYySFctrDEgidAwMTMOOTAwMDAeFwOwMDAxMDEwMDAwMDBaFwOzMDAxMDEw
MDAwMDBaMCIxIDAeBgNVBAMTF1A2NjJIVy1EMSAgMDAxMzQ5MDAwMDAxMFwwDQYJ
KoZIhvcNAQEBBQADSwAwSAJBABE2AsjRsfw3EOk6IQL3rG2P+/M0qpwWukomFnB5
X7nLrI4k6Bnq18mILg4b5rxBh/0OyJK1OEVJYSJ8JGm/PeOCAwEAAeNNMEswDgYD
VROPAQEABAQDAgKkMCUGA1UdEQQeMBjAwMTMOOTAwMDAwMUBhdXRvLmdlbi5j
ZXJOMBiGA1UdEwEBAAQIMAYBaf8CAQEwDQYJKoZIhvcNAQEFBQADQQBcpmg/f5dHQ
jLkoBBkhlmfeQOB511d08w2+I3gsufnomEUHbMye6XDK1LV6wi3FkkLb5isJuhtT/
o/zpeIY1ypo6
-----END CERTIFICATE-----
```

The following table describes the labels in this screen.

**Table 119** My Certificate Details

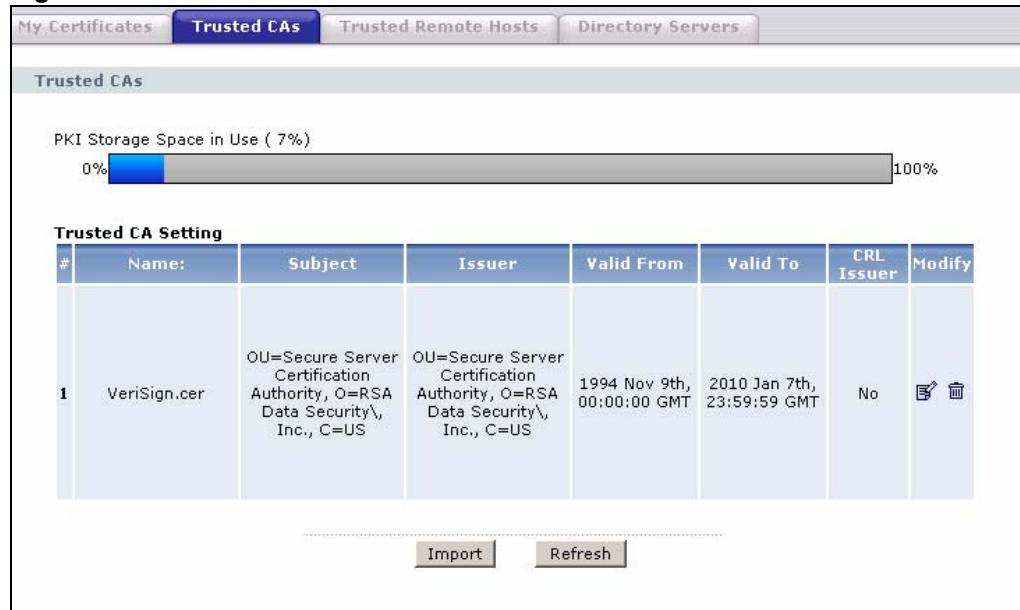
LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this certificate. You may use any character (not including spaces).
Property Default self-signed certificate which signs the imported remote host certificates.	Select this check box to have the ZyXEL Device use this certificate to sign the trusted remote host certificates that you import to the ZyXEL Device. This check box is only available with self-signed certificates. If this check box is already selected, you cannot clear it in this screen, you must select this check box in another self-signed certificate's details screen. This automatically clears the check box in the details screen of the certificate that was previously set to sign the imported trusted remote host certificates.
Certification Path	Click the <b>Refresh</b> button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself). If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The ZyXEL Device does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click <b>Refresh</b> to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority or generated by the ZyXEL Device.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same as the <b>Subject Name</b> field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. The ZyXEL Device uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyXEL Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).

**Table 119** My Certificate Details (continued)

LABEL	DESCRIPTION
Subject Alternative Name	This field displays the certificate owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the SHA1 algorithm.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment. You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export	Click this button and then <b>Save</b> in the <b>File Download</b> screen. The <b>Save As</b> screen opens, browse to the location that you want to use and click <b>Save</b> .
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device. You can only change the name, except in the case of a self-signed certificate, which you can also set to be the default self-signed certificate that signs the imported trusted remote host certificates.
Cancel	Click <b>Cancel</b> to quit and return to the <b>My Certificates</b> screen.

## 19.8 Trusted CAs

Click **Security > Certificates > Trusted CAs** to open the **Trusted CAs** screen. This screen displays a summary list of certificates of the certification authorities that you have set the ZyXEL Device to accept as trusted. The ZyXEL Device accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

**Figure 174** Trusted CAs

The following table describes the labels in this screen.

**Table 120** Trusted CAs

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyXEL Device's PKI storage space that is currently in use. The bar turns from blue to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the <b>Subject</b> field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
CRL Issuer	This field displays Yes if the certification authority issues Certificate Revocation Lists for the certificates that it has issued and you have selected the <b>Issues certificate revocation lists (CRL)</b> check box in the certificate's details screen to have the ZyXEL Device check the CRL before trusting any certificates issued by the certification authority. Otherwise the field displays "No".

**Table 120** Trusted CAs (continued)

LABEL	DESCRIPTION
Modify	Click the details icon to open a screen with an in-depth list of information about the certificate. Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificates. Note that subsequent certificates move up by one when you take this action.
Import	Click <b>Import</b> to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the ZyXEL Device.
Refresh	Click this button to display the current validity status of the certificates.

## 19.9 Trusted CA Import

Click **Security > Certificates > Trusted CAs** to open the **Trusted CAs** screen and then click **Import** to open the **Trusted CA Import** screen. Follow the instructions in this screen to save a trusted certification authority's certificate to the ZyXEL Device.



You must remove any spaces from the certificate's filename before you can import the certificate.

**Figure 175** Trusted CA Import

**Certificates - Trusted CAs - Import**

Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7

File Path:

The following table describes the labels in this screen.

**Table 121** Trusted CA Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse</b> to find it.
Browse	Click <b>Browse</b> to find the certificate file you want to upload.
Apply	Click <b>Apply</b> to save the certificate on the ZyXEL Device.
Cancel	Click <b>Cancel</b> to quit and return to the <b>Trusted CAs</b> screen.

## 19.10 Trusted CA Details

Click **Security > Certificates > Trusted CAs** to open the **Trusted CAs** screen. Click the details icon to open the **Trusted CA Details** screen. Use this screen to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the ZyXEL Device to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

**Figure 176** Trusted CA Details



The following table describes the labels in this screen.

**Table 122** Trusted CA Details

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Property Issues certificate revocation lists (CRLs)	Select this check box to have the ZyXEL Device check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL). Clear this check box to have the ZyXEL Device not check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL).
Certification Path	Click the <b>Refresh</b> button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the end entity's own certificate). The ZyXEL Device does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click <b>Refresh</b> to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same information as in the <b>Subject Name</b> field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyXEL Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).

**Table 122** Trusted CA Details (continued)

LABEL	DESCRIPTION
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
CRL Distribution Points	This field displays how many directory servers with Lists of revoked certificates the issuing certification authority of this certificate makes available. This field also displays the domain names or IP addresses of the servers.
MD5 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
SHA1 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form.  You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export	Click this button and then <b>Save</b> in the <b>File Download</b> screen. The <b>Save As</b> screen opens, browse to the location that you want to use and click <b>Save</b> .
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device. You can only change the name and/or set whether or not you want the ZyXEL Device to check the CRL that the certification authority issues before trusting a certificate issued by the certification authority.
Cancel	Click <b>Cancel</b> to quit and return to the <b>Trusted CAs</b> screen.

## 19.11 Trusted Remote Hosts

Click **Security > Certificates > Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen. This screen displays a list of the certificates of peers that you trust but which are not signed by one of the certification authorities on the **Trusted CAs** screen.

You do not need to add any certificate that is signed by one of the certification authorities on the **Trusted CAs** screen since the ZyXEL Device automatically accepts any valid certificate signed by a trusted certification authority as being trustworthy.

**Figure 177** Trusted Remote Hosts

The following table describes the labels in this screen.

**Table 123** Trusted Remote Hosts

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyXEL Device's PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
Issuer (My Default Self-signed Certificate)	This field displays identifying information about the default self-signed certificate on the ZyXEL Device that the ZyXEL Device uses to sign the trusted remote host certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Modify	Click the details icon to open a screen with an in-depth list of information about the certificate. Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.
Import	Click <b>Import</b> to open a screen where you can save the certificate of a remote host (which you trust) from your computer to the ZyXEL Device.
Refresh	Click this button to display the current validity status of the certificates.

## 19.12 Verifying a Trusted Remote Host's Certificate

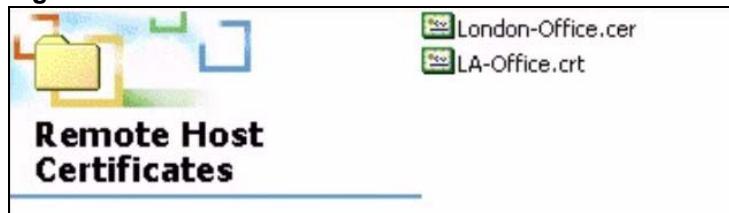
Certificates issued by certification authorities have the certification authority's signature for you to check. Self-signed certificates only have the signature of the host itself. This means that you must be very careful when deciding to import (and thereby trust) a remote host's self-signed certificate.

### 19.12.1 Trusted Remote Host Certificate Fingerprints

A certificate's fingerprints are message digests calculated using the MD5 or SHA1 algorithms. The following procedure describes how to use a certificate's fingerprint to verify that you have the remote host's actual certificate.

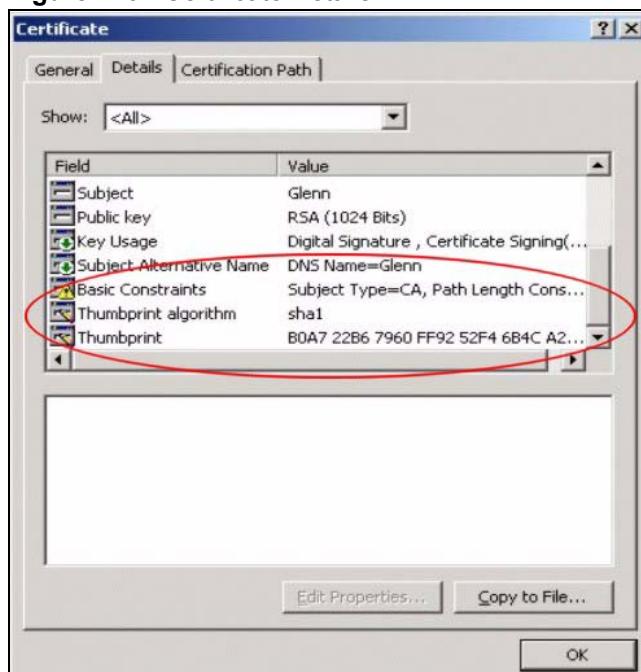
- 1 Browse to where you have the remote host's certificate saved on your computer.
- 2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

**Figure 178** Remote Host Certificates



- 3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

**Figure 179** Certificate Details



Verify (over the phone for example) that the remote host has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields.

## 19.13 Trusted Remote Hosts Import

Click **Security > Certificates > Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen and then click **Import** to open the **Trusted Remote Host Import** screen. Follow the instructions in this screen to save a trusted host's certificate to the ZyXEL Device.



The trusted remote host certificate must be a self-signed certificate; and you must remove any spaces from its filename before you can import it.

**Figure 180** Trusted Remote Host Import

Certificates - Trusted Remote Hosts - Import

Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7

File Path:

The following table describes the labels in this screen.

**Table 124** Trusted Remote Host Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse</b> to find it.
Browse	Click <b>Browse</b> to find the certificate file you want to upload.
Apply	Click <b>Apply</b> to save the certificate on the ZyXEL Device.
Cancel	Click <b>Cancel</b> to quit and return to the <b>Trusted Remote Hosts</b> screen.

## 19.14 Trusted Remote Host Certificate Details

Click **Security > Certificates > Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen. Click the details icon to open the **Trusted Remote Host Details** screen. Use this screen to view in-depth information about the trusted remote host's certificate and/or change the certificate's name.

**Figure 181** Trusted Remote Host Details

The following table describes the labels in this screen.

**Table 125** Trusted Remote Host Details

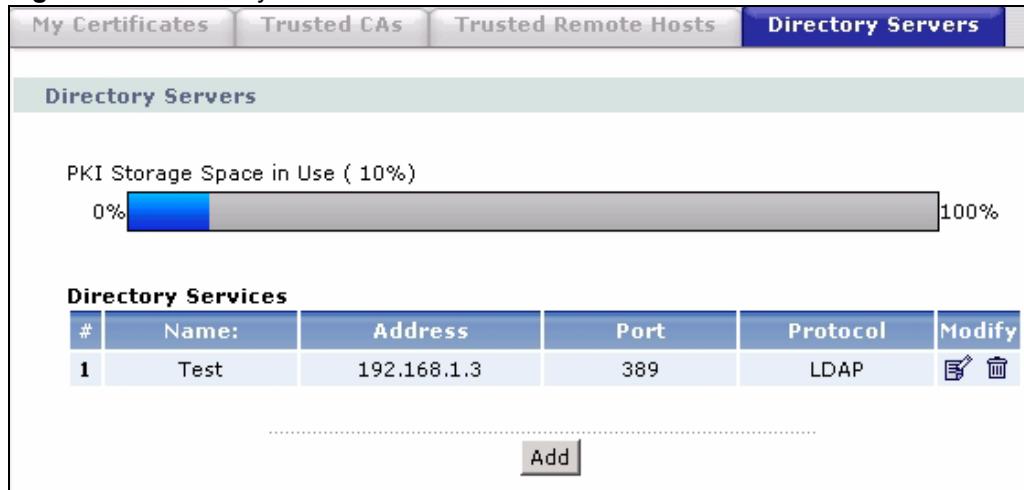
LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Certification Path	Click the <b>Refresh</b> button to have this read-only text box display the end entity's own certificate and a list of certification authority certificates in the hierarchy of certification authorities that validate a certificate's issuing certification authority. For a trusted host, the list consists of the end entity's own certificate and the default self-signed certificate that the ZyXEL Device uses to sign remote host certificates.
Refresh	Click <b>Refresh</b> to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. With trusted remote host certificates, this field always displays CA-signed. The ZyXEL Device is the Certification Authority that signed the certificate. X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the device that created the certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the default self-signed certificate on the ZyXEL Device that the ZyXEL Device uses to sign the trusted remote host certificates.
Signature Algorithm	This field displays the type of algorithm that the ZyXEL Device used to sign the certificate, which is rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyXEL Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.

**Table 125** Trusted Remote Host Details (continued)

LABEL	DESCRIPTION
MD5 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the MD5 algorithm. You cannot use this value to verify that this is the remote host's actual certificate because the ZyXEL Device has signed the certificate; thus causing this value to be different from that of the remote hosts actual certificate. See <a href="#">Section 19.12 on page 318</a> for how to verify a remote host's certificate.
SHA1 Fingerprint	This is the certificate's message digest that the ZyXEL Device calculated using the SHA1 algorithm. You cannot use this value to verify that this is the remote host's actual certificate because the ZyXEL Device has signed the certificate; thus causing this value to be different from that of the remote hosts actual certificate. See <a href="#">Section 19.12 on page 318</a> for how to verify a remote host's certificate.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export	Click this button and then <b>Save</b> in the <b>File Download</b> screen. The <b>Save As</b> screen opens, browse to the location that you want to use and click <b>Save</b> .
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device. You can only change the name of the certificate.
Cancel	Click <b>Cancel</b> to quit configuring this screen and return to the <b>Trusted Remote Hosts</b> screen.

## 19.15 Directory Servers

Click **Security > Certificates > Directory Servers** to open the **Directory Servers** screen. This screen displays a summary list of directory servers (that contain lists of valid and revoked certificates) that have been saved into the ZyXEL Device. If you decide to have the ZyXEL Device check incoming certificates against the issuing certification authority's list of revoked certificates, the ZyXEL Device first checks the server(s) listed in the **CRL Distribution Points** field of the incoming certificate. If the certificate does not list a server or the listed server is not available, the ZyXEL Device checks the servers listed here.

**Figure 182** Directory Servers

The following table describes the labels in this screen.

**Table 126** Directory Servers

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyXEL Device's PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	The index number of the directory server. The servers are listed in alphabetical order.
Name	This field displays the name used to identify this directory server.
Address	This field displays the IP address or domain name of the directory server.
Port	This field displays the port number that the directory server uses.
Protocol	This field displays the protocol that the directory server uses.
Modify	Click the details icon to open a screen where you can change the information about the directory server. Click the delete icon to remove the directory server entry. A window displays asking you to confirm that you want to delete the directory server. Note that subsequent certificates move up by one when you take this action.
Add	Click <b>Add</b> to open a screen where you can configure information about a directory server so that the ZyXEL Device can access it.

## 19.16 Directory Server Add and Edit

Click **Security > Certificates > Directory Servers** to open the **Directory Servers** screen. Click **Add** (or the details icon) to open the **Directory Server Add** screen. Use this screen to configure information about a directory server that the ZyXEL Device can access.

**Figure 183** Directory Server Add and Edit

**Directory Service Setting**

Name:

Access protocol: **LDAP**

Server address:  (Host Name or IP Address)

Server port:

**Login Setting**

Login:

Password:

**Buttons:** Back | Apply | Cancel

The following table describes the labels in this screen.

**Table 127** Directory Server Add and Edit

LABEL	DESCRIPTION
Directory Service Setting	
Name	Type up to 31 ASCII characters (spaces are not permitted) to identify this directory server.
Access Protocol	Use the drop-down list box to select the access protocol used by the directory server. <b>LDAP</b> (Lightweight Directory Access Protocol) is a protocol over TCP that specifies how clients access directories of certificates and lists of revoked certificates. <sup>1</sup>
Server Address	Type the IP address (in dotted decimal notation) or the domain name of the directory server.
Server Port	This field displays the default server port number of the protocol that you select in the <b>Access Protocol</b> field. You may change the server port number if needed, however you must use the same server port number that the directory server uses. 389 is the default server port number for LDAP.
Login Setting	
Login	The ZyXEL Device may need to authenticate itself in order to assess the directory server. Type the login name (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority).
Back	Click <b>Back</b> to return to the <b>Directory Servers</b> screen.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to quit configuring this screen.

1. At the time of writing, LDAP is the only choice of directory server access protocol.

---

# PART VI

# Advanced

---

- Static Route (327)
- Bandwidth Management (331)
- Dynamic DNS Setup (339)
- Remote Management Configuration (343)
- Universal Plug-and-Play (UPnP) (361)



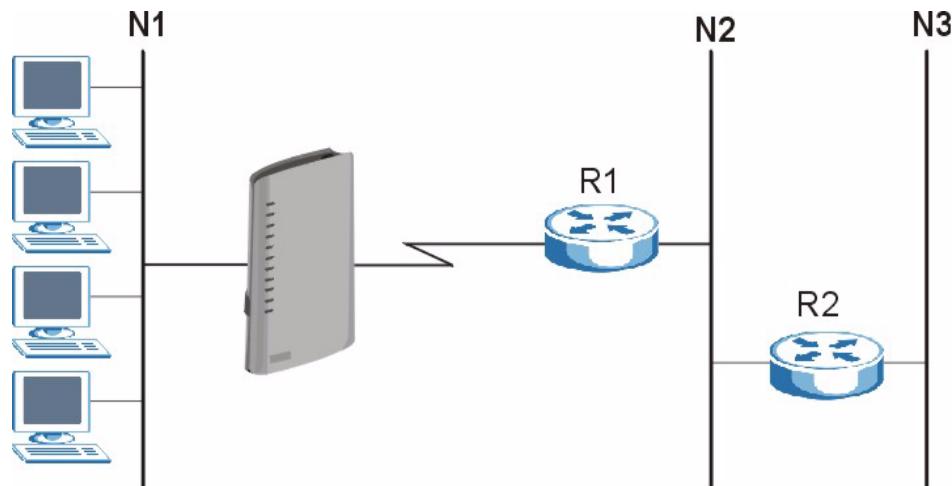
# Static Route

This chapter shows you how to configure static routes for your ZyXEL Device.

## 20.1 Static Route

Each remote node specifies only the network to which the gateway is directly connected, and the ZyXEL Device has no knowledge of the networks beyond. For instance, the ZyXEL Device knows about network N2 in the following figure through remote node Router 1. However, the ZyXEL Device is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node Router 1 (via gateway Router 2). The static routes are for you to tell the ZyXEL Device about the networks beyond the remote nodes.

**Figure 184** Example of Static Routing Topology



## 20.2 Configuring Static Route

Click **Advanced > Static Route** to open the **Static Route** screen.

**Figure 185** Static Route

Static Route Rules						
#	Active	Name	Destination	Netmask	Gateway	Modify
1	-	-	-	-	-	
2	-	-	-	-	-	
3	-	-	-	-	-	
4	-	-	-	-	-	
5	-	-	-	-	-	
6	-	-	-	-	-	
7	-	-	-	-	-	
8	-	-	-	-	-	
9	-	-	-	-	-	
10	-	-	-	-	-	
11	-	-	-	-	-	
12	-	-	-	-	-	
13	-	-	-	-	-	
14	-	-	-	-	-	
15	-	-	-	-	-	
16	-	-	-	-	-	

**Apply**    **Cancel**

The following table describes the labels in this screen.

**Table 128** Static Route

LABEL	DESCRIPTION
#	This is the number of an individual static route.
Active	This field shows whether this static route is active ( <b>Yes</b> ) or not ( <b>No</b> ).
Name	This is the name that describes or identifies this route.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Netmask	This parameter specifies the IP network subnet mask of the final destination.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Modify	Click the edit icon to go to the screen where you can set up a static route on the ZyXEL Device. Click the delete icon to remove a static route from the ZyXEL Device. A window displays asking you to confirm that you want to delete the route.
Apply	Click this to apply your changes to the ZyXEL Device.
Cancel	Click this to return to the previously saved configuration.

### 20.2.1 Static Route Edit

Select a static route index number and click **Edit**. The screen shown next appears. Use this screen to configure the required information for a static route.

**Figure 186** Static Route Edit

The screenshot shows a 'Static Route Setup' window. At the top is a header bar with the title. Below it is a form area containing five input fields. The first field, 'Active', has a checked checkbox. The other four fields have the value '0.0.0.0'. At the bottom of the form are three buttons: 'Back', 'Apply', and 'Cancel'.

The following table describes the labels in this screen.

**Table 129** Static Route Edit

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Back	Click <b>Back</b> to return to the previous screen without saving.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.



# Bandwidth Management

This chapter contains information about configuring bandwidth management, editing rules and viewing the ZyXEL Device's bandwidth management logs.

## 21.1 Bandwidth Management Overview

ZyXEL's Bandwidth Management allows you to specify bandwidth management rules based on application. You can allocate specific amounts of bandwidth capacity (bandwidth budgets) to different bandwidth rules.

The ZyXEL Device applies bandwidth management to traffic that it forwards out through an interface. The ZyXEL Device does not control the bandwidth of traffic that comes into an interface.

Bandwidth management applies to all traffic flowing out of the router, regardless of the traffic's source.

Traffic redirect or IP alias may cause LAN-to-LAN traffic to pass through the ZyXEL Device and be managed by bandwidth management.

## 21.2 Application-based Bandwidth Management

You can create bandwidth classes based on individual applications (like Web, FTP and E-mail, for example).

## 21.3 Auto Classifier

Automatic Traffic Classifier (ATC) is a bandwidth management tool that prioritizes data packets sent across the network. ATC assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Voice over IP or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

ATC assigns priority based on packet size, since time-sensitive applications such as Internet telephony (Voice over IP or VoIP) tend to have smaller packet sizes than non-time sensitive applications such as FTP (File Transfer Protocol). The following table shows some common applications, their time sensitivity, and their typical data packet sizes. Note that the figures given are merely examples - sizes may differ according to application and circumstances.

**Table 130** Typical Packet Sizes

APPLICATION	TIME SENSITIVITY	TYPICAL PACKET SIZE (BYTES)
Voice over IP (SIP)	High	< 250
Online Gaming	High	60 ~ 90
Web browsing (http)	Medium	300 ~ 600
FTP	Low	1500

When ATC is activated, the device sends traffic with smaller packets before traffic with larger packets if the network is congested.

ATC assigns priority to packets as shown in the following table.

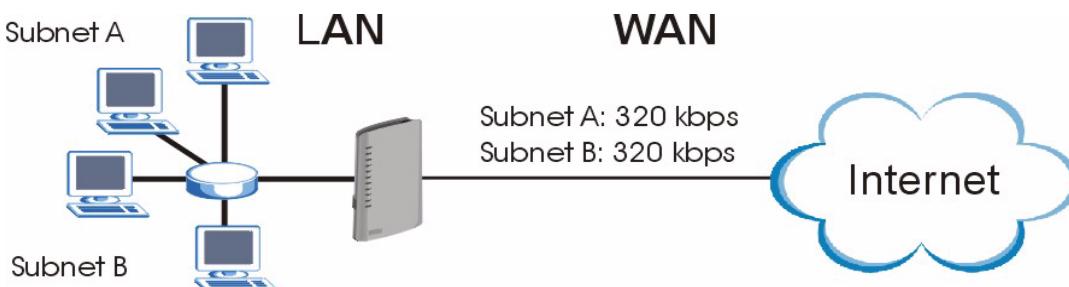
**Table 131** Automatic Traffic Classifier Priorities

PACKET SIZE (BYTES)	ATC PRIORITY
1 ~ 250	ATC_High
250 ~ 1100	ATC_Medium
1100 +	ATC_Low

## 21.4 Subnet-based Bandwidth Management

You can create bandwidth classes based on subnets.

The following figure shows LAN subnets. You could configure one bandwidth class for subnet A and another for subnet B.

**Figure 187** Subnet-based Bandwidth Management Example

## 21.5 Application and Subnet-based Bandwidth Management

You could also create bandwidth classes based on a combination of a subnet and an application. The following example table shows bandwidth allocations for application specific traffic from separate LAN subnets.

**Table 132** Application and Subnet-based Bandwidth Management Example

TRAFFIC TYPE	FROM SUBNET A	FROM SUBNET B
VoIP (SIP)	64 Kbps	64 Kbps
Web	64 Kbps	64 Kbps
FTP	64 Kbps	64 Kbps
E-mail	64 Kbps	64 Kbps

### 21.5.1 Bandwidth Management Priorities

Traffic with a higher priority gets through faster while traffic with a lower priority is dropped if the network is congested. The following table describes the priorities that you can apply to traffic that the ZyXEL Device forwards out through an interface.

**Table 133** Bandwidth Management Priorities

PRIORITY	DESCRIPTION
High	Typically used for voice traffic or video that is especially sensitive to jitter (variations in delay).
Mid	Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay.
Low	This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users.

## 21.6 Configuring Bandwidth Management (General)

Click **Advanced > Bandwidth MGMT** to open the screen as shown next.

Use this screen to enable or disable bandwidth management, and to enable or disable automatic traffic classification.

**Figure 188** Bandwidth Management: General

General	Rule Setup	Monitor
<b>Bandwidth Management</b> <input checked="" type="checkbox"/> Active <input checked="" type="checkbox"/> Auto Classifier <b>Note :</b> Automatically assign the packet to predefined classes depending on the packet size.		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

The following table describes the labels in this screen.

**Table 134** Bandwidth Management: General

LABEL	DESCRIPTION
Active	Select the check box to enable bandwidth management.
Auto Classifier	Select the check box to enable Automatic Traffic Classifier (ATC). ATC assigns each packet to a bandwidth management class based on its size, since time-sensitive applications such as VoIP tend to have smaller packet sizes than non-time sensitive applications such as FTP. When ATC is enabled, traffic with a smaller packet size is assigned a higher priority than traffic with a larger packet size.
Apply	Click <b>Apply</b> to save your settings back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 21.7 Bandwidth Management Rule Setup

You must use the **Bandwidth Management General** screen to enable bandwidth management before you can configure rules.

Click **Advanced > Bandwidth MGMT > Rule Setup** to open the following screen.

**Figure 189** Bandwidth Management: Rule Setup

General	Rule Setup	Monitor										
<b>Rule Setup</b> Direction: LAN    Service: WWW    Priority: High    Bandwidth: 10 (kbps)    Add												
<b>To LAN Interface</b> <table border="1"> <thead> <tr> <th>#</th> <th>Active</th> <th>Rule Name</th> <th>Destination Port</th> <th>Priority</th> <th>Bandwidth(kbps)</th> <th>Modify</th> </tr> </thead> </table>						#	Active	Rule Name	Destination Port	Priority	Bandwidth(kbps)	Modify
#	Active	Rule Name	Destination Port	Priority	Bandwidth(kbps)	Modify						
Apply    Cancel												

The following table describes the labels in this screen.

**Table 135** Bandwidth Management: Rule Setup

LABEL	DESCRIPTION
Direction	Select <b>LAN</b> to apply bandwidth management to traffic that the ZyXEL Device forwards to the LAN. Select <b>WAN</b> to apply bandwidth management to traffic that the ZyXEL Device forwards to the WAN. Select <b>WLAN</b> to apply bandwidth management to traffic that the ZyXEL Device forwards to the WLAN.
Service	Select a service for your rule or you can select <b>User define</b> to go to the screen where you can define your own.
Priority	Select a priority from the drop down list box. Choose <b>High</b> , <b>Mid</b> or <b>Low</b> .

**Table 135** Bandwidth Management: Rule Setup (continued)

LABEL	DESCRIPTION
Bandwidth (kbps)	Specify the maximum bandwidth allowed for the rule in kbps. The recommendation is a setting between 20 kbps and 20000 kbps for an individual rule. If you want to leave some bandwidth for traffic that does not match a bandwidth filter, make sure that the interface's root class has more bandwidth than the sum of the bandwidths of the interface's bandwidth management rules.
Add	Click this button to save your rule. It displays in the following table.
#	This is the number of an individual bandwidth management rule.
Rule Name	This is the name of the rule.
Destination Port	This is the port number of the destination. 0 means any destination port.
Priority	This is the priority of this rule.
Bandwidth (kbps)	This is the maximum bandwidth allowed for the rule in kbps.
Modify	Click the Edit icon to go to the screen where you can edit the rule. Click the Remove icon to delete an existing rule.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 21.7.1 Rule Configuration

Click the **Edit** icon or **User defined** in the **Service** field to configure a bandwidth management rule. Use bandwidth rules to allocate specific amounts of bandwidth capacity (bandwidth budgets) to specific applications and/or subnets.

**Figure 190** Bandwidth Management Rule Configuration

The screenshot shows the 'Rule Configuration' screen. At the top, there is a 'Rule Configuration' section with fields for 'Rule Name' (set to 'WWW'), 'BW Budget' (set to '10 (Kbps)'), 'Priority' (set to 'High'), and a checked checkbox for 'Use All Managed Bandwidth'. Below this is a 'Filter Configuration' section with fields for 'Service' (set to 'User defined'), 'Destination Address' (set to '0.0.0.0'), 'Destination Subnet Netmask' (set to '0.0.0.0'), 'Destination Port' (set to '0'), 'Source Address' (set to '0.0.0.0'), 'Source Subnet Netmask' (set to '0.0.0.0'), 'Source Port' (set to '80'), and 'Protocol' (set to 'TCP'). At the bottom of the screen are three buttons: 'Back', 'Apply', and 'Cancel'.

See [Appendix E](#) on page 475 for a list of commonly-used services.

The following table describes the labels in this screen.

**Table 136** Bandwidth Management Rule Configuration

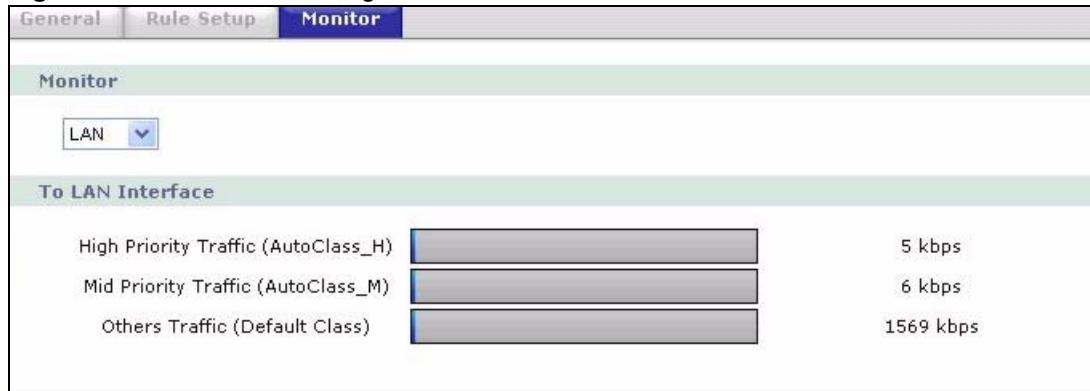
LABEL	DESCRIPTION
Rule Configuration	
Rule Name	Use the auto-generated name or enter a descriptive name of up to 20 alphanumeric characters, including spaces.
BW Budget	Specify the maximum bandwidth allowed for the rule in kbps. The recommendation is a setting between 20 kbps and 20000 kbps for an individual rule.
Priority	Select a priority from the drop down list box. Choose <b>High</b> , <b>Mid</b> or <b>Low</b> .
Use All Managed Bandwidth	Select this option to allow a rule to borrow unused bandwidth on the interface. Bandwidth borrowing is governed by the priority of the rules. That is, a rule with the highest priority is the first to borrow bandwidth. Do not select this if you want to leave bandwidth available for other traffic types or if you want to restrict the amount of bandwidth that can be used for the traffic that matches this rule.
Filter Configuration	
Service	<p>This field simplifies bandwidth class configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the bandwidth filter fields (other than enabling or disabling the filter).</p> <p>SIP (Session Initiation Protocol) is a signaling protocol used in Internet telephony, instant messaging and other VoIP (Voice over IP) applications. Select <b>SIP</b> from the drop-down list box to configure this bandwidth filter for traffic that uses SIP.</p> <p>File Transfer Protocol (FTP) is an Internet file transfer service that operates on the Internet and over TCP/IP networks. A system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files. Select <b>FTP</b> from the drop-down list box to configure this bandwidth filter for FTP traffic.</p> <p>H.323 is a standard teleconferencing protocol suite that provides audio, data and video conferencing. It allows for real-time point-to-point and multipoint communication between client computers over a packet-based network that does not provide a guaranteed quality of service. Select <b>H.323</b> from the drop-down list box to configure this bandwidth filter for traffic that uses H.323.</p> <p>Select <b>User defined</b> from the drop-down list box if you do not want to use a predefined application for the bandwidth class. When you select <b>User defined</b>, you need to configure at least one of the following fields (other than the <b>Subnet Mask</b> fields which you only enter if you also enter a corresponding destination or source IP address).</p>
Destination Address	Enter the destination IP address in dotted decimal notation.
Destination Subnet Netmask	Enter the destination subnet mask. This field is N/A if you do not specify a <b>Destination Address</b> . Refer to the appendix for more information on IP subnetting.
Destination Port	Enter the port number of the destination. See <a href="#">Appendix E on page 475</a> for some common services and port numbers. A blank destination IP address means any destination IP address.
Source Address	Enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Source Subnet Netmask	Enter the destination subnet mask. This field is N/A if you do not specify a <b>Source Address</b> . Refer to the appendix for more information on IP subnetting. A blank source port means any source port number.

**Table 136** Bandwidth Management Rule Configuration (continued)

LABEL	DESCRIPTION
Source Port	Enter the port number of the source. See <a href="#">Appendix E on page 475</a> for some common services and port numbers.
Protocol	Select the protocol (TCP or UDP) or select User defined and enter the protocol (service type) number. 0 means any protocol number.
Back	Click <b>Back</b> to go to the previous screen.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 21.8 Bandwidth Monitor

To view the ZyXEL Device's bandwidth usage, click **Advanced > Bandwidth MGMT > Monitor**. The screen appears as shown. Select an interface from the drop-down list box to view the bandwidth usage of its bandwidth rules. The gray section of the bar represents the percentage of unused bandwidth and the blue color represents the percentage of bandwidth in use.

**Figure 191** Bandwidth Management: Monitor



# Dynamic DNS Setup

This chapter discusses how to configure your ZyXEL Device to use Dynamic DNS.

## 22.1 Dynamic DNS Overview

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

### 22.1.1 DYNDNS Wildcard

Enabling the wildcard feature for your host causes \*.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

See [Section 22.2 on page 339](#) for configuration instruction.

## 22.2 Configuring Dynamic DNS

To change your ZyXEL Device's DDNS, click **Advanced > Dynamic DNS**. The screen appears as shown.

See [Section 22.1 on page 339](#) for more information.

**Figure 192** Dynamic DNS

Active Dynamic DNS

Service Provider: WWW.DynDNS.ORG

Dynamic DNS Type: Dynamic DNS

Host Name:

User Name:

Password:

Enable Wildcard Option

Enable off line option (Only applies to custom DNS)

**IP Address Update Policy**

Use WAN IP Address

Dynamic DNS server auto detect IP Address

Use specified IP Address: 0.0.0.0

Apply Cancel

The following table describes the fields in this screen.

**Table 137** Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Active Dynamic DNS	Select this check box to use dynamic DNS.
Service Provider	This is the name of your Dynamic DNS service provider.
Dynamic DNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Name	Type the domain name assigned to your ZyXEL Device by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
User Name	Type your user name.
Password	Type the password assigned to you.
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard.
Enable off line option	This option is available when <b>CustomDNS</b> is selected in the <b>DDNS Type</b> field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
IP Address Update Policy	
Use WAN IP Address	Select this option to update the IP address of the host name(s) to the WAN IP address.

**Table 137** Dynamic DNS (continued)

LABEL	DESCRIPTION
Dynamic DNS server auto detect IP Address	Select this option only when there are one or more NAT routers between the ZyXEL Device and the DDNS server. This feature has the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address.  Note: The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the ZyXEL Device and the DDNS server.
Use specified IP Address	Type the IP address of the host name(s). Use this if you have a static IP address.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.



# Remote Management Configuration

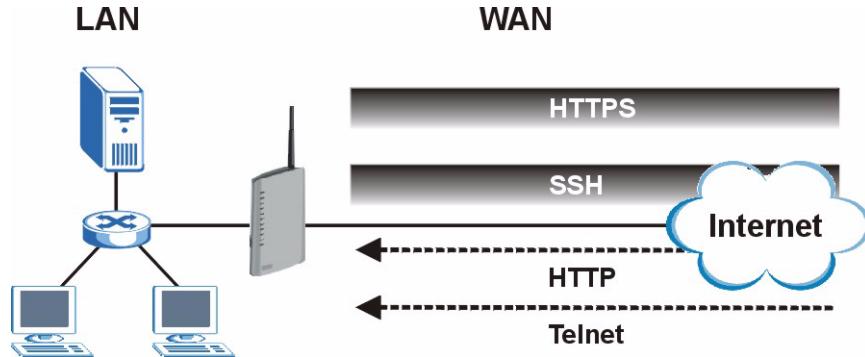
This chapter provides information on configuring remote management.

## 23.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which ZyXEL Device interface (if any) from which computers.

The following figure shows secure and insecure management of the ZyXEL Device coming in from the WAN. HTTPS and SSH access are secure. HTTP and Telnet access are not secure.

**Figure 193** Secure and Insecure Remote Management From the WAN



When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access.

You may manage your ZyXEL Device from a remote location via:

- Internet (WAN only)
- ALL (LAN and WAN)
- LAN only,
- Neither (Disable).



When you choose **WAN only** or **LAN & WAN**, you still need to configure a firewall rule to allow access.

---

To disable remote management of a service, select **Disable** in the corresponding **Access Status** field.

You may only have one remote management session running at a time. The ZyXEL Device automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

- 1** SSH
- 1** Telnet
- 2** HTTPS and HTTP

### 23.1.1 Remote Management Limitations

Remote management does not work when:

- You have not enabled that service on the interface in the corresponding remote management screen.
- You have disabled that service in one of the remote management screens.
- The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the ZyXEL Device will disconnect the session immediately.
- There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
- There is a firewall rule that blocks it.

### 23.1.2 Remote Management and NAT

When NAT is enabled:

- Use the ZyXEL Device's WAN IP address when configuring from the WAN.
- Use the ZyXEL Device's LAN IP address when configuring from the LAN.

### 23.1.3 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The ZyXEL Device automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

## 23.2 Introduction to HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

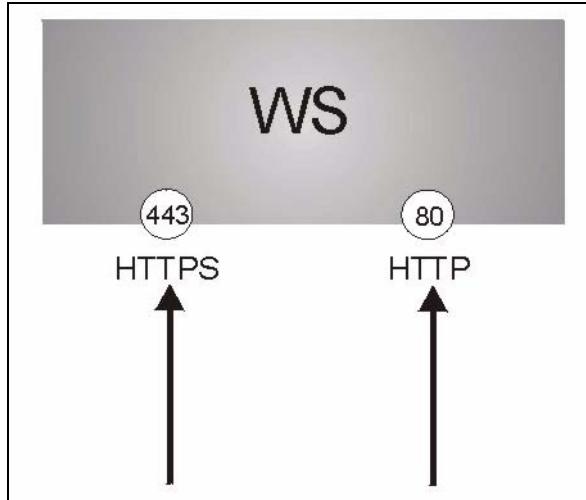
It relies upon certificates, public keys, and private keys (see [Chapter 19 on page 301](#) for more information).

HTTPS on the ZyXEL Device is used so that you may securely access the ZyXEL Device using the web configurator. The SSL protocol specifies that the SSL server (the ZyXEL Device) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyXEL Device), whereas the SSL client only should authenticate itself when the SSL server requires it to do so (select **Authenticate Client Certificates** in the **REMOTE MGMT, HTTP** screen). **Authenticate Client Certificates** is optional and if selected means the SSL-client must send the ZyXEL Device a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the ZyXEL Device.

Please refer to the following figure.

- 1** HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the ZyXEL Device's WS (web server).
- 2** HTTP connection requests from a web browser go to port 80 (by default) on the ZyXEL Device's WS (web server).

**Figure 194** HTTPS Implementation



If you disable **HTTP Server Access (Disable)** in the **REMOTE MGMT HTTP** screen, then the ZyXEL Device blocks all HTTP connection attempts.

### 23.3 HTTP

To change your ZyXEL Device's World Wide Web settings, click **Advanced > Remote MGMT** to display the **HTTP** screen.

**Figure 195** Remote Management: HTTP

The screenshot shows the 'HTTP' tab selected in the top navigation bar. Below it, there are two main sections: 'HTTP' and 'HTTPS'.  
**HTTP Section:**  
- Port: 80  
- Access Status: LAN & WAN (selected)  
- Secured Client IP: Radio button set to 'All'  
**HTTPS Section:**  
- Server Host Key: auto\_generated\_self\_signed\_cert (See [My Certificates](#))  
- Authenticate Client Certificates: Unchecked  
- Port: 443  
- Access Status: LAN & WAN (selected)  
- Secured Client IP: Radio button set to 'All'  
**Note:**  
1: For [UPnP](#) to function normally, the HTTP service must be available for LAN computers using UPnP.  
2: You may also need to create a [Firewall](#) rule  
At the bottom right are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

**Table 138** Remote Management: HTTP

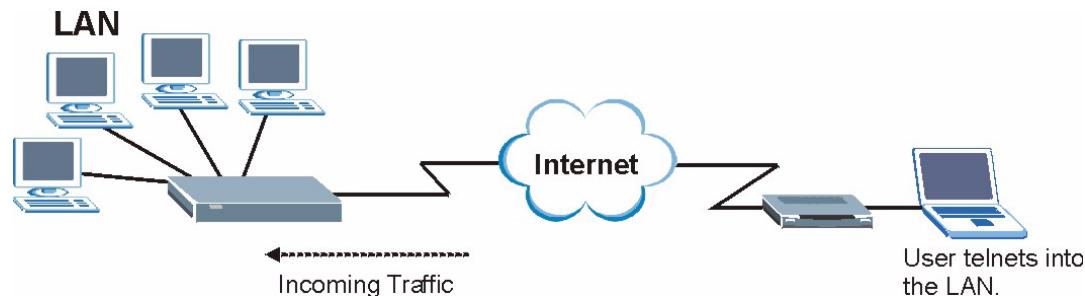
LABEL	DESCRIPTION
HTTP	
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	A secured client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select <b>All</b> to allow any computer to access the ZyXEL Device using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
HTTPS	
Server Host Key	Select the certificate that the ZyXEL Device will use to identify itself. The ZyXEL Device is the SSL server and must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyXEL Device).
Authenticate Client Certificates	Select <b>Authenticate Client Certificates</b> (optional) to require the SSL client to authenticate itself to the ZyXEL Device by sending the ZyXEL Device a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the ZyXEL Device (see <a href="#">Section Chapter 19</a> on <a href="#">page 301</a> on importing certificates for details).
Port	The HTTPS proxy server listens on port 443 by default. If you change the HTTPS proxy server port to a different number on the ZyXEL Device, for example 8443, then you must notify people who need to access the ZyXEL Device web configurator to use “https://ZyXEL Device IP Address: <b>8443</b> ” as the URL.

**Table 138** Remote Management: HTTP

LABEL	DESCRIPTION
Access Status	Select a ZyXEL Device interface from <b>Access Status</b> on which incoming HTTPS access is allowed. You can allow only secure web configurator access by setting the <b>HTTP Access Status</b> field to <b>Disable</b> and setting the <b>HTTPS Access Status</b> field to an interface(s).
Secure Client IP	A secure client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select <b>All</b> to allow any computer to access the ZyXEL Device using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click <b>Apply</b> to save your settings back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 23.4 Telnet

You can configure your ZyXEL Device for remote Telnet access as shown next. The administrator uses Telnet from a computer on a remote network to access the ZyXEL Device.

**Figure 196** Telnet Configuration on a TCP/IP Network

## 23.5 Configuring Telnet

Click **Advanced > Remote MGMT > Telnet** tab to display the screen as shown.

**Figure 197** Remote Management: Telnet

The following table describes the labels in this screen.

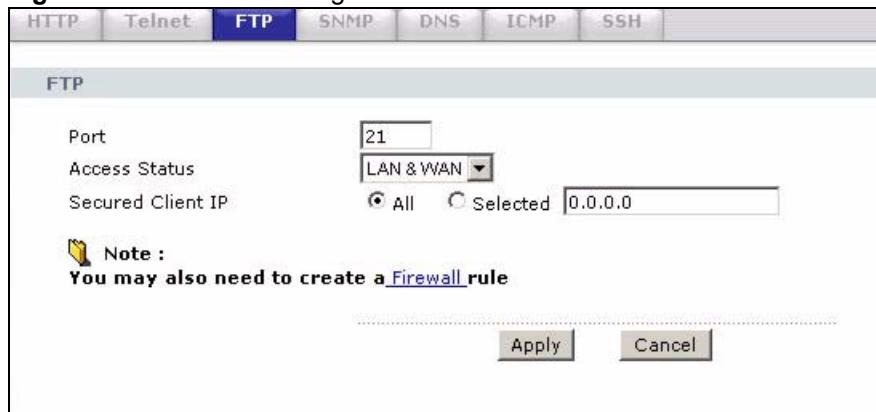
**Table 139** Remote Management: Telnet

LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	A secured client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select <b>All</b> to allow any computer to access the ZyXEL Device using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 23.6 Configuring FTP

You can upload and download the ZyXEL Device’s firmware and configuration files using FTP. Please see [Section 29.7 on page 413](#) for details. To use this feature, your computer must have an FTP client.

To change your ZyXEL Device’s FTP settings, click **Advanced > Remote MGMT > FTP** tab. The screen appears as shown.

**Figure 198** Remote Management: FTP

The following table describes the labels in this screen.

**Table 140** Remote Management: FTP

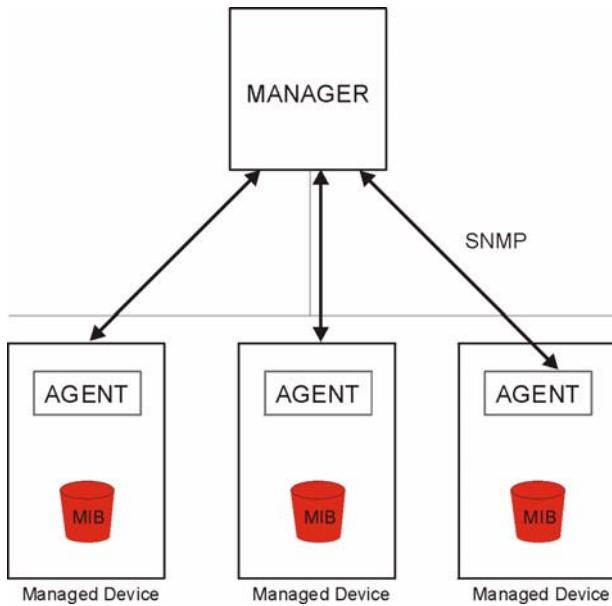
LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	A secured client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select <b>All</b> to allow any computer to access the ZyXEL Device using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 23.7 SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyXEL Device supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyXEL Device through the network. The ZyXEL Device supports SNMP version one (SNMPv1) and version two (SNMPv2). The next figure illustrates an SNMP management operation.



SNMP is only available if TCP/IP is configured.

**Figure 199** SNMP Management Model

An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the ZyXEL Device). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

### 23.7.1 Supported MIBs

The ZyXEL Device supports MIB II, which is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

### 23.7.2 SNMP Traps

The ZyXEL Device will send traps to the SNMP manager when any one of the following events occurs:

**Table 141** SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
0	coldStart (defined in RFC-1215)	A trap is sent after booting (power on).
1	warmStart (defined in RFC-1215)	A trap is sent after booting (software reboot).
4	authenticationFailure (defined in RFC-1215)	A trap is sent to the manager when receiving any SNMP get or set requirements with the wrong community (password).
6	whyReboot (defined in ZYXEL-MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot:	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CI command "sys reboot", etc.).
6b	For fatal error:	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

### 23.7.3 Configuring SNMP

To change your ZyXEL Device's SNMP settings, click **Advanced > Remote MGMT > SNMP**. The screen appears as shown.

**Figure 200** Remote Management: SNMP

HTTP	Telnet	FTP	SNMP	DNS	ICMP	SSH
<b>SNMP</b>						
Port	161					
Access Status	LAN & WAN					
Secured Client IP	<input type="radio"/> All <input checked="" type="radio"/> Selected 0.0.0.0					
<b>SNMP Configuration</b>						
Get Community	public					
Set Community	public					
Trap Community	public					
Trap Destination	0.0.0.0					
<b>Note :</b> You may also need to create a <a href="#">Firewall rule</a>						
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>						

The following table describes the labels in this screen.

**Table 142** Remote Management: SNMP

LABEL	DESCRIPTION
<b>SNMP</b>	
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	A secured client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select <b>All</b> to allow any computer to access the ZyXEL Device using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
<b>SNMP Configuration</b>	
Get Community	Enter the <b>Get Community</b> , which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the <b>Set community</b> , which is the password for incoming Set requests from the management station. The default is public and allows all requests.
<b>Trap</b>	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the station to send your SNMP traps to.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 23.8 Configuring DNS

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. Refer to [Chapter 8 on page 117](#) for background information.

To change your ZyXEL Device’s DNS settings, click **Advanced > Remote MGMT > DNS**. The screen appears as shown. Use this screen to set from which IP address the ZyXEL Device will accept DNS queries and on which interface it can send them your ZyXEL Device’s DNS settings.

**Figure 201** Remote Management: DNS

The following table describes the labels in this screen.

**Table 143** Remote Management: DNS

LABEL	DESCRIPTION
Port	The DNS service port number is 53 and cannot be changed here.
Access Status	Select the interface(s) through which a computer may send DNS queries to the ZyXEL Device.
Secured Client IP	A secured client is a “trusted” computer that is allowed to send DNS queries to the ZyXEL Device. Select <b>All</b> to allow any computer to send DNS queries to the ZyXEL Device. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to send DNS queries to the ZyXEL Device.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

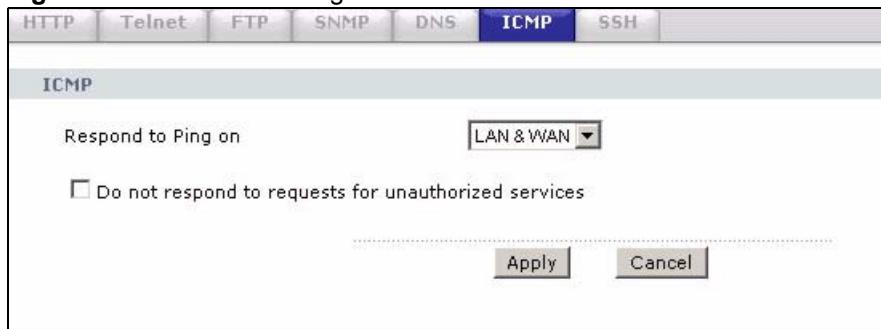
## 23.9 Configuring ICMP

To change your ZyXEL Device’s security settings, click **Advanced > Remote MGMT > ICMP**. The screen appears as shown.

If an outside user attempts to probe an unsupported port on your ZyXEL Device, an ICMP response packet is automatically returned. This allows the outside user to know the ZyXEL Device exists. Your ZyXEL Device supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your ZyXEL Device when unsupported ports are probed.



If you want your device to respond to pings and requests for unauthorized services, you may also need to configure the firewall anti probing settings to match.

**Figure 202** Remote Management: ICMP

The following table describes the labels in this screen.

**Table 144** Remote Management: ICMP

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The ZyXEL Device will not respond to any incoming Ping requests when <b>Disable</b> is selected. Select <b>LAN</b> to reply to incoming LAN Ping requests. Select <b>WAN</b> to reply to incoming WAN Ping requests. Otherwise select <b>LAN &amp; WAN</b> to reply to both incoming LAN and WAN Ping requests.
Do not respond to requests for unauthorized services	Select this option to prevent hackers from finding the ZyXEL Device by probing for unused ports. If you select this option, the ZyXEL Device will not respond to port request(s) for unused ports, thus leaving the unused ports and the ZyXEL Device unseen. By default this option is not selected and the ZyXEL Device will reply with an ICMP Port Unreachable packet for a port probe on its unused UDP ports, and a TCP Reset packet for a port probe on its unused TCP ports.  Note that the probing packets must first traverse the ZyXEL Device's firewall mechanism before reaching this anti-probing mechanism. Therefore if the firewall mechanism blocks a probing packet, the ZyXEL Device reacts based on the corresponding firewall policy to send a TCP reset packet for a blocked TCP packet or an ICMP port-unreachable packet for a blocked UDP packets or just drop the packets without sending a response packet.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 23.10 SSH

You can use SSH (Secure SHell) to securely access the ZyXEL Device's command line interface. Specify which interfaces allow SSH access and from which IP address the access can come.

Unlike Telnet or FTP, which transmit data in plaintext (clear or unencrypted text), SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network. In the following figure, computer A on the Internet uses SSH to securely connect to the WAN port of the ZyXEL Device for a management session.

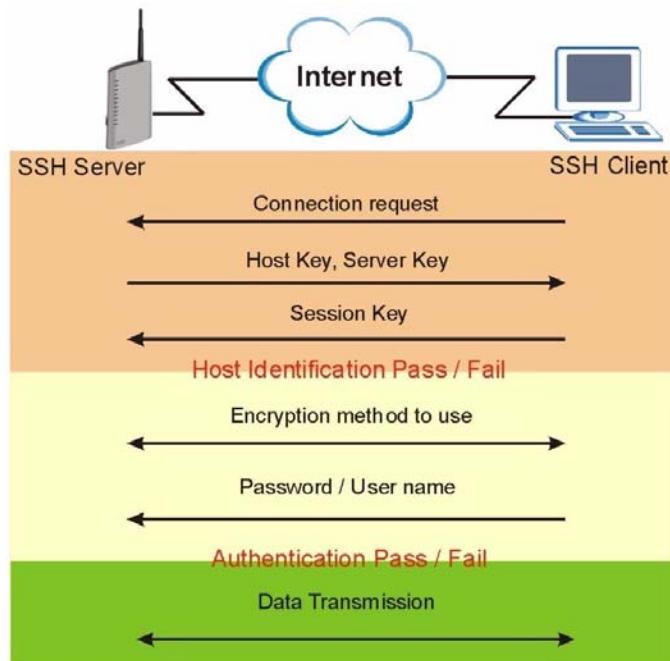
**Figure 203** SSH Communication Over the WAN Example  
WAN



## 23.11 How SSH Works

The following table summarizes how a secure connection is established between two remote hosts.

**Figure 204** How SSH Works



### 1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

### 2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

### 3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

## 23.12 SSH Implementation on the ZyXEL Device

Your ZyXEL Device supports SSH version 1.5 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the ZyXEL Device for remote SMT management and file transfer on port 22. Only one SSH connection is allowed at a time.

### 23.12.1 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the ZyXEL Device over SSH.

## 23.13 Configuring SSH

Click **ADVANCED > REMOTE MGMT > SSH** to change your ZyXEL Device's Secure Shell settings.



It is recommended that you disable Telnet and FTP when you configure SSH for secure connections.

**Figure 205** ADVANCED > REMOTE MGMT > SSH

The following table describes the labels in this screen.

**Table 145** ADVANCED > REMOTE MGMT > SSH

LABEL	DESCRIPTION
Server Host Key	Select the certificate whose corresponding private key is to be used to identify the ZyXEL Device for SSH connections. You must have certificates already configured in the <b>My Certificates</b> screen (Click <b>My Certificates</b> and see <a href="#">Section 19.4 on page 303</a> for details).
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.

**Table 145** ADVANCED > REMOTE MGMT > SSH

LABEL	DESCRIPTION
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secure Client IP	A secure client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select <b>All</b> to allow any computer to access the ZyXEL Device using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 23.14 Secure Telnet Using SSH Examples

This section shows two examples using a command interface and a graphical interface SSH client program to remotely access the ZyXEL Device. The configuration and connection steps are similar for most SSH client programs. Refer to your SSH client program user’s guide.

### 23.14.1 Example 1: Microsoft Windows

This section describes how to access the ZyXEL Device using the Secure Shell Client program.

- 1 Launch the SSH client and specify the connection information (IP address, port number or device name) for the ZyXEL Device.
- 2 Configure the SSH client to accept connection using SSH version 1.
- 3 A window displays prompting you to store the host key in your computer. Click **Yes** to continue.

**Figure 206** SSH Example 1: Store Host Key

Enter the password to log in to the ZyXEL Device. The SMT main menu displays next.

### 23.14.2 Example 2: Linux

This section describes how to access the ZyXEL Device using the OpenSSH client program that comes with most Linux distributions.

- 1 Test whether the SSH service is available on the ZyXEL Device.

Enter “telnet 192.168.1.1 22” at a terminal prompt and press [ENTER]. The computer attempts to connect to port 22 on the ZyXEL Device (using the default IP address of 192.168.1.1).

A message displays indicating the SSH protocol version supported by the ZyXEL Device.

**Figure 207** SSH Example 2: Test

```
$ telnet 192.168.1.1 22
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^].
SSH-1.5-1.0.0
```

- 2** Enter “ssh -1 192.168.1.1”. This command forces your computer to connect to the ZyXEL Device using SSH version 1. If this is the first time you are connecting to the ZyXEL Device using SSH, a message displays prompting you to save the host information of the ZyXEL Device. Type “yes” and press [ENTER].

Then enter the password to log in to the ZyXEL Device.

**Figure 208** SSH Example 2: Log in

```
$ ssh -1 192.168.1.1
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be
established.
RSA1 key fingerprint is
21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.1' (RSA1) to the list of
known hosts.
Administrator@192.168.1.1's password:
```

- 3** The SMT main menu displays next.

## 23.15 Secure FTP Using SSH Example

This section shows an example on file transfer using the OpenSSH client program. The configuration and connection steps are similar for other SSH client programs. Refer to your SSH client program user’s guide.

- 1** Enter “sftp -1 192.168.1.1”. This command forces your computer to connect to the ZyXEL Device for secure file transfer using SSH version 1. If this is the first time you are connecting to the ZyXEL Device using SSH, a message displays prompting you to save the host information of the ZyXEL Device. Type “yes” and press [ENTER].
- 2** Enter the password to login to the ZyXEL Device.
- 3** Use the “put” command to upload a new firmware to the ZyXEL Device.

**Figure 209** Secure FTP: Firmware Upload Example

```
$ sftp -l 192.168.1.1
Connecting to 192.168.1.1...
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be
established.
RSA1 key fingerprint is
21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.1' (RSA1) to the list of
known hosts.
Administrator@192.168.1.1's password:
sftp> put firmware.bin ras
Uploading firmware.bin to /ras
Read from remote host 192.168.1.1: Connection reset by peer
Connection closed
$
```



# Universal Plug-and-Play (UPnP)

This chapter introduces the UPnP feature in the web configurator.

## 24.1 Introducing Universal Plug and Play

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

See [Section 24.2.1 on page 362](#) for configuration instructions.

### 24.1.1 How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

### 24.1.2 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the NAT chapter for more information on NAT.

### 24.1.3 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the ZyXEL Device allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

## 24.2 UPnP and ZyXEL

ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

See the following sections for examples of installing and using UPnP.

### 24.2.1 Configuring UPnP

Click **Advanced > UPnP** to display the screen shown next.

See [Section 24.1 on page 361](#) for more information.

**Figure 210** Configuring UPnP



The following table describes the fields in this screen.

**Table 146** Configuring UPnP

LABEL	DESCRIPTION
Active the Universal Plug and Play (UPnP) Feature	Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the ZyXEL Device's IP address (although you must still enter the password to access the web configurator).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the ZyXEL Device so that they can communicate through the ZyXEL Device, for example by using NAT traversal. UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.

**Table 146** Configuring UPnP

LABEL	DESCRIPTION
Allow UPnP to pass through Firewall	Select this check box to allow traffic from UPnP-enabled applications to bypass the firewall. Clear this check box to have the firewall block all UPnP application packets (for example, MSN packets).
Apply	Click <b>Apply</b> to save the setting to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to return to the previously saved settings.

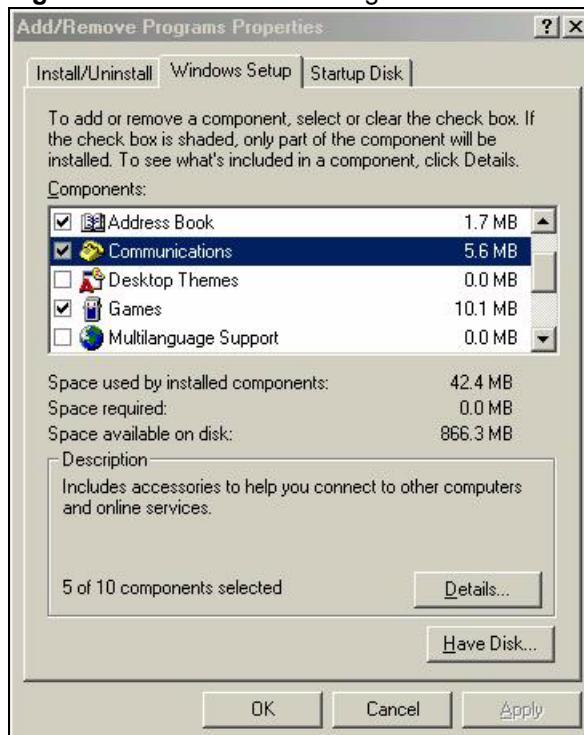
## 24.3 Installing UPnP in Windows Example

This section shows how to install UPnP in Windows Me and Windows XP.

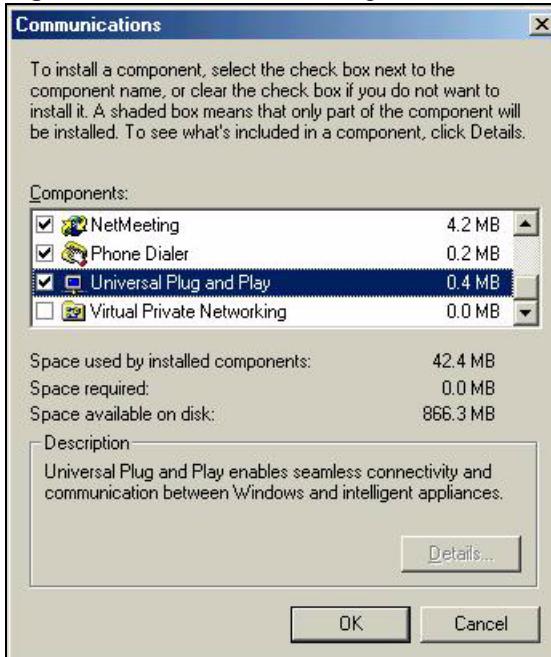
### Installing UPnP in Windows Me

Follow the steps below to install the UPnP in Windows Me.

- 1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.
- 2 Click on the **Windows Setup** tab and select **Communication** in the Components selection box. Click **Details**.

**Figure 211** Add/Remove Programs: Windows Setup: Communication

- 3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

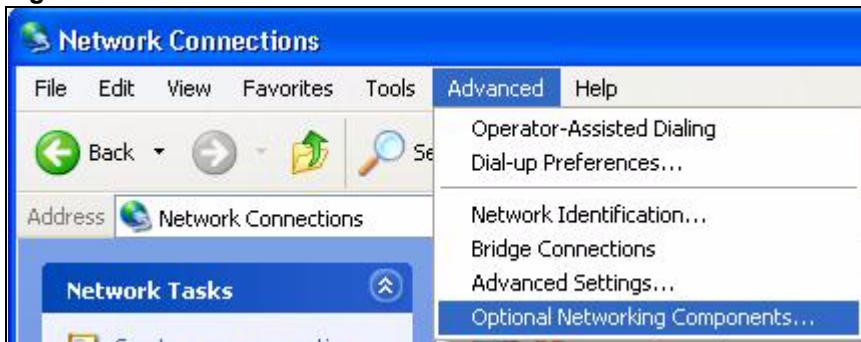
**Figure 212** Add/Remove Programs: Windows Setup: Communication: Components

- 4** Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.
- 5** Restart the computer when prompted.

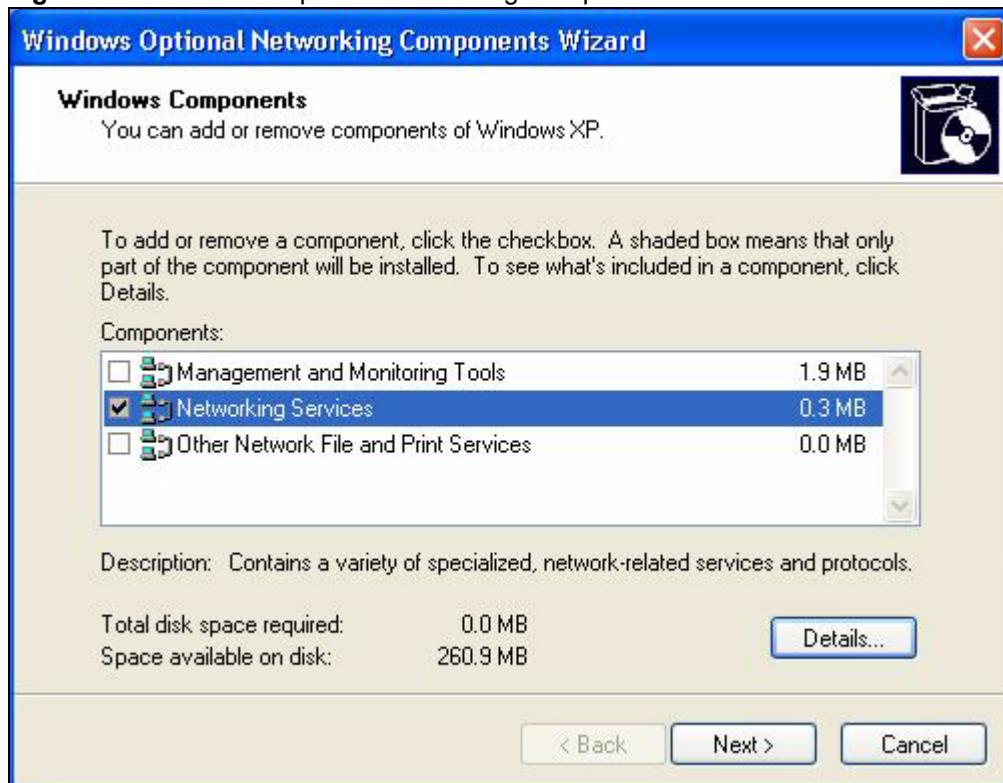
### Installing UPnP in Windows XP

Follow the steps below to install the UPnP in Windows XP.

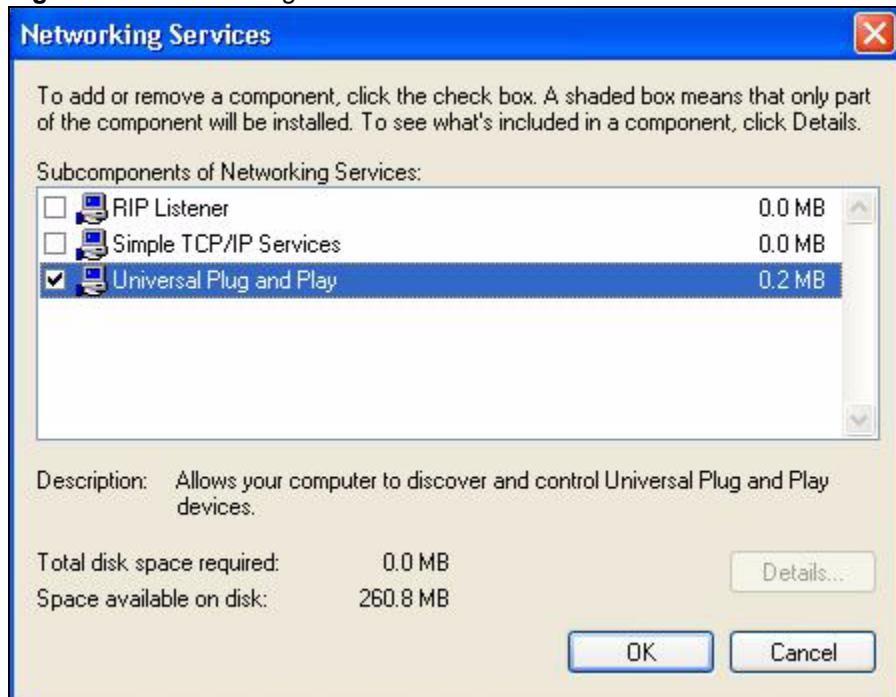
- 1** Click **Start** and **Control Panel**.
- 2** Double-click **Network Connections**.
- 3** In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ....**

**Figure 213** Network Connections

- 4** The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

**Figure 214** Windows Optional Networking Components Wizard

- 5 In the **Networking Services** window, select the **Universal Plug and Play** check box.

**Figure 215** Networking Services

- 6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

## 24.4 Using UPnP in Windows XP Example

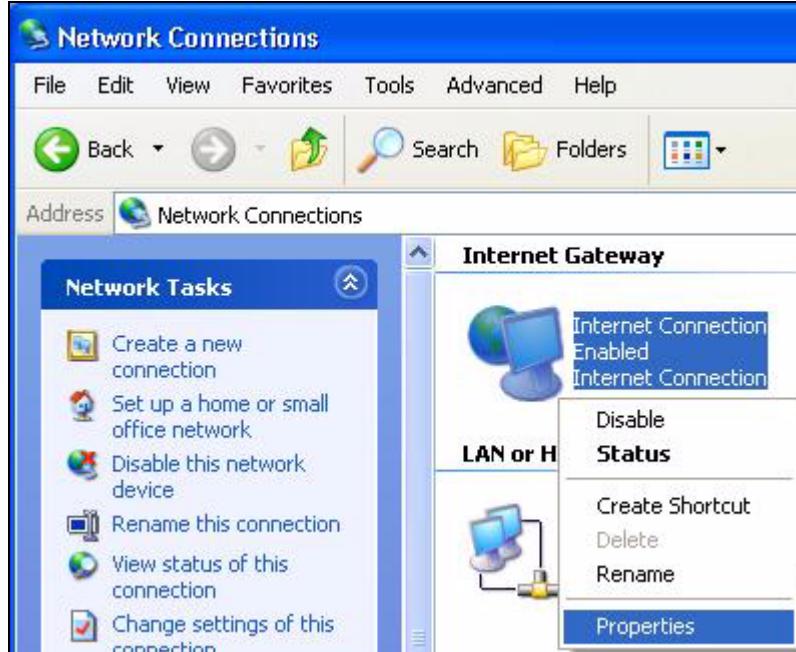
This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the ZyXEL Device.

Make sure the computer is connected to a LAN port of the ZyXEL Device. Turn on your computer and the ZyXEL Device.

### Auto-discover Your UPnP-enabled Network Device

- 1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.
- 2 Right-click the icon and select **Properties**.

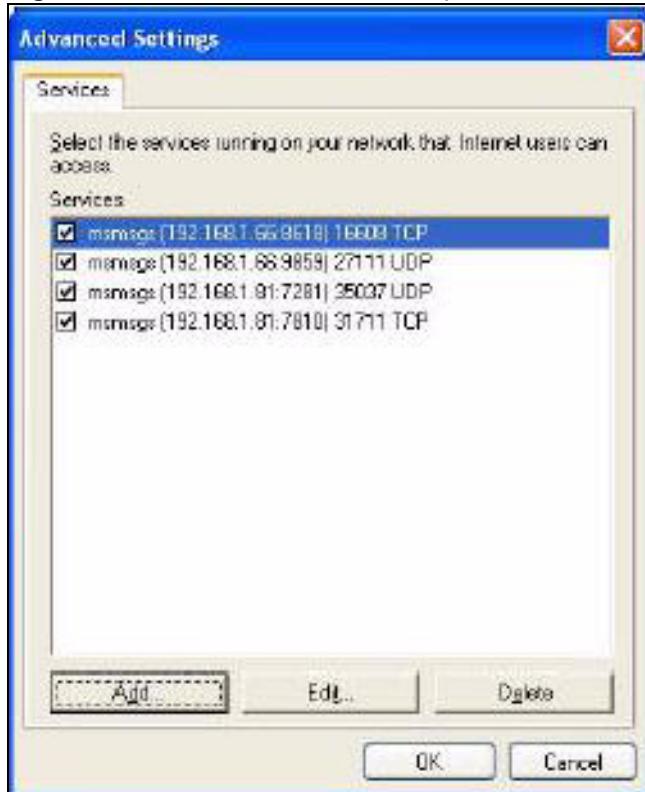
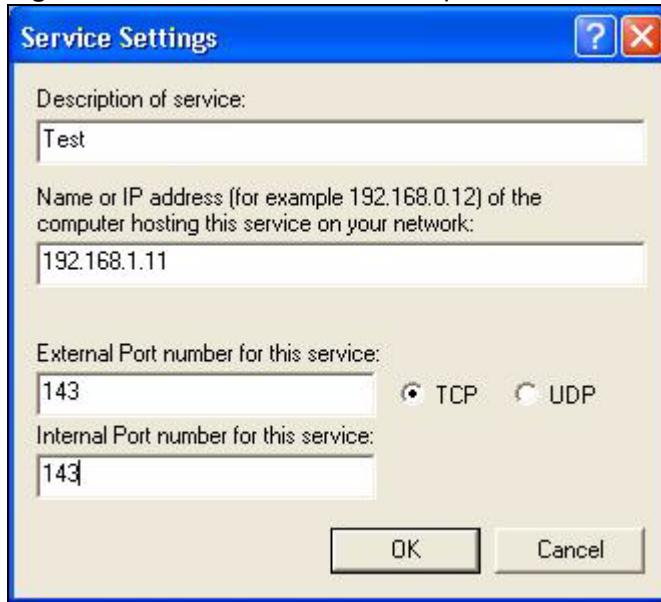
**Figure 216** Network Connections



- 3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

**Figure 217** Internet Connection Properties

- 4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

**Figure 218** Internet Connection Properties: Advanced Settings**Figure 219** Internet Connection Properties: Advanced Settings: Add

- 5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.
- 6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

**Figure 220** System Tray Icon

**7** Double-click on the icon to display your current Internet connection status.

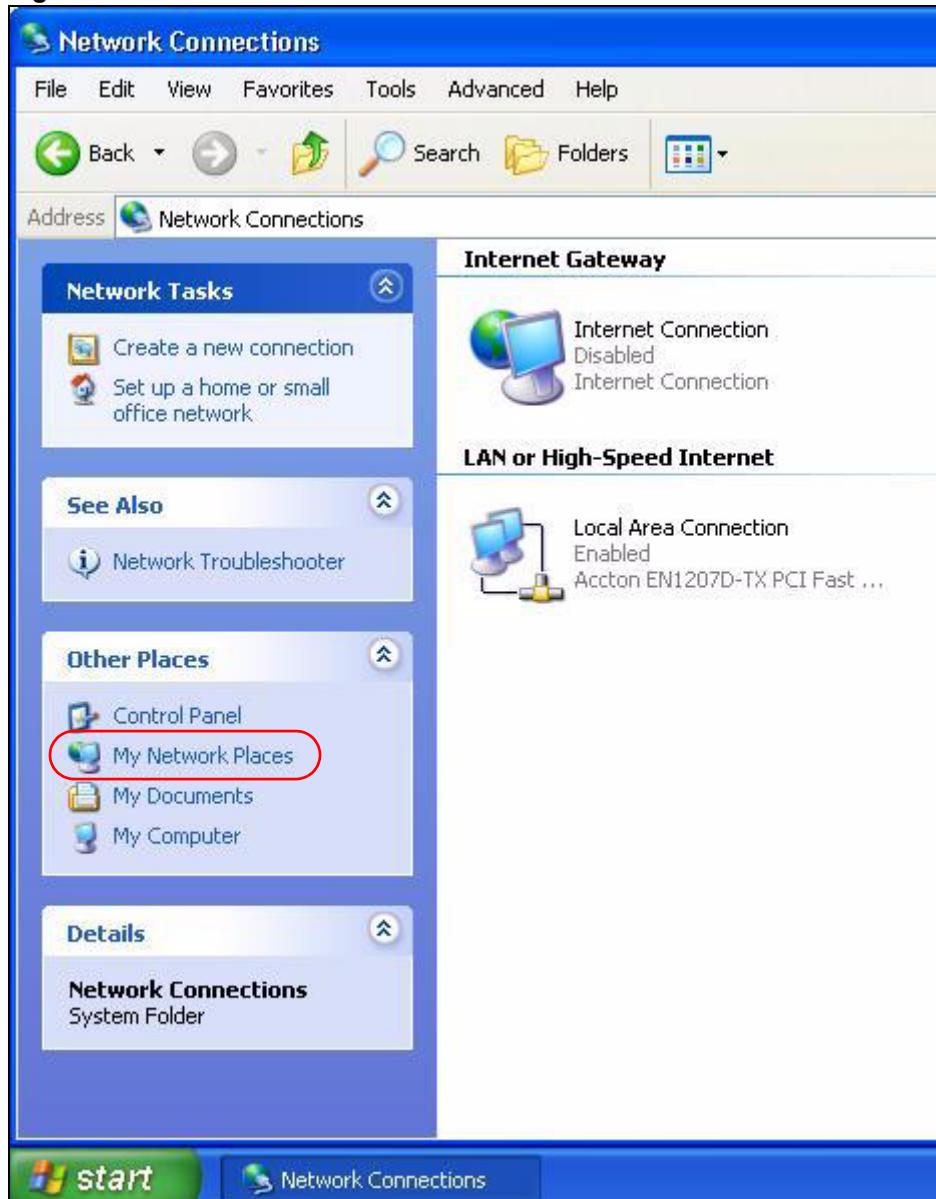
**Figure 221** Internet Connection Status

### Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the ZyXEL Device without finding out the IP address of the ZyXEL Device first. This comes helpful if you do not know the IP address of the ZyXEL Device.

Follow the steps below to access the web configurator.

- 1** Click **Start** and then **Control Panel**.
- 2** Double-click **Network Connections**.
- 3** Select **My Network Places** under **Other Places**.

**Figure 222** Network Connections

- 4 An icon with the description for each UPnP-enabled device displays under **Local Network**.
- 5 Right-click on the icon for your ZyXEL Device and select **Invoke**. The web configurator login screen displays.

**Figure 223** Network Connections: My Network Places

- 6 Right-click on the icon for your ZyXEL Device and select **Properties**. A properties window displays with basic information about the ZyXEL Device.

**Figure 224** Network Connections: My Network Places: Properties: Example



---

# PART VII

# Maintenance and Troubleshooting

---

System (375)  
Call History (381)  
Logs (387)  
Troubleshooting (401)  
Tools (407)  
Diagnostic (419)  
Product Specifications (423)



# System

Use this screen to configure the ZyXEL Device's time and date settings.

## 25.1 General Setup and System Name

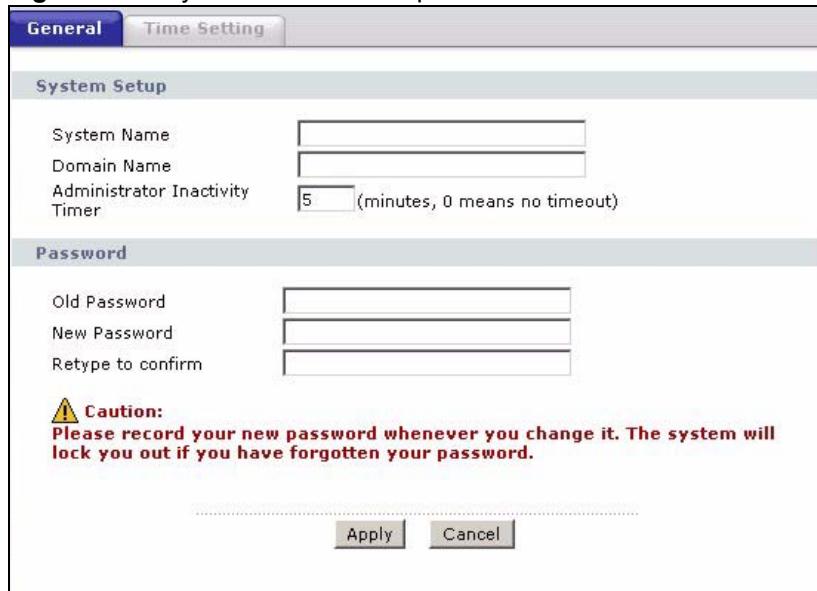
**General Setup** contains administrative and system-related information. **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

- In Windows 95/98 click **Start, Settings, Control Panel, Network**. Click the Identification tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start, Settings, Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **start, My Computer, View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the ZyXEL Device **System Name**.

### 25.1.1 General Setup

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name), the domain name can be assigned from the ZyXEL Device via DHCP.

Click **Maintenance > System** to open the **General** screen.

**Figure 225** System General Setup

The following table describes the labels in this screen.

**Table 147** System General Setup

LABEL	DESCRIPTION
General Setup	
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator or telnet) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Password	
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the ZyXEL Device.
Retype to Confirm	Type the new password again for confirmation.
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 25.2 Time Setting

To change your ZyXEL Device's time and date, click **Maintenance > System > Time Setting**. The screen appears as shown. Use this screen to configure the ZyXEL Device's time based on your local time zone.

**Figure 226** System Time Setting

The following table describes the fields in this screen.

**Table 148** System Time Setting

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your ZyXEL Device. Each time you reload this page, the ZyXEL Device synchronizes the time with the time server.
Current Date	This field displays the date of your ZyXEL Device. Each time you reload this page, the ZyXEL Device synchronizes the date with the time server.
Time and Date Setup	

**Table 148** System Time Setting (continued)

LABEL	DESCRIPTION
Manual	<p>Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.</p> <p>When you enter the time settings manually, the ZyXEL Device uses the new setting once you click <b>Apply</b>.</p> <p><b>Note:</b> If you enter time settings manually, they revert to their defaults when power is lost.</p>
New Time (hh:mm:ss)	<p>This field displays the last updated time from the time server or the last time configured manually.</p> <p>When you set <b>Time and Date Setup</b> to <b>Manual</b>, enter the new time in this field and then click <b>Apply</b>.</p>
New Date (yyyy/mm/dd)	<p>This field displays the last updated date from the time server or the last date configured manually.</p> <p>When you set <b>Time and Date Setup</b> to <b>Manual</b>, enter the new date in this field and then click <b>Apply</b>.</p>
Get from Time Server	Select this radio button to have the ZyXEL Device get the time and date from the time server you specified below.
Time Protocol	<p>Select the time service protocol that your time server sends when you turn on the ZyXEL Device. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works.</p> <p>The main difference between them is the format.</p> <p><b>Daytime (RFC 867)</b> format is day/month/year/time zone of the server.</p> <p><b>Time (RFC 868)</b> format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.</p> <p>The default, <b>NTP (RFC 1305)</b>, is similar to Time (RFC 868).</p>
Time Server Address	Enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	<p>Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.</p> <p>Select this option if you use Daylight Saving Time.</p>
Start Date	<p>Configure the day and time when Daylight Saving Time starts if you selected <b>Enable Daylight Saving</b>. The <b>o'clock</b> field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>Second, Sunday, March and 2:00</b>.</p> <p>Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>Last, Sunday, March</b>. The time you type in the <b>o'clock</b> field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>

**Table 148** System Time Setting (continued)

LABEL	DESCRIPTION
End Date	Configure the day and time when Daylight Saving Time ends if you selected <b>Enable Daylight Saving</b> . The <b>o'clock</b> field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>First, Sunday, November</b> and <b>2:00</b> . Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>Last, Sunday, October</b> . The time you type in the <b>o'clock</b> field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click <b>Apply</b> to save your changes back to the ZyXEL Device.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.



# Call History

This chapter contains information about configuring call history settings and viewing the Zyxel Device's phone call records.

## 26.1 Call History Overview

Call history chronicles incoming and outgoing PSTN and VoIP calls. You can choose the frequency with which the Zyxel Device saves details of phone calls, and send these records to an administrator (as e-mail) or to a mail server.

This feature allows you to trace all of your PSTN and VoIP call records and see details of how many calls you missed, dialed and received. You can also see call timers showing how much time you spend on PSTN and VoIP calls.



---

The Call History feature does not record details of internal calls.

---

## 26.2 Viewing the Call History Summary

Use the **Summary** screen to see the duration and packet statistics of incoming and outgoing PSTN calls and VoIP calls in the following time periods: **today**, **yesterday**, **last week** and **last month**.

Click **Maintenance > Call History > Summary**. The following screen displays.

**Figure 227** Call History > Summary

Summary	Call History	Call History Settings				
<b>Summary of Call History</b>						
Type of Summary	Start Time	End Time	Tx Packets	Rx Packets	Duration of PSTN	Duration of VoIP
Today	01/01/2000	01/01/2000	0	0	0:00:00	0:00:17
Yesterday	12/31/1999	12/31/1999	0	0	0:00:00	0:00:00
Last Week	N/A	N/A	0	0	0:00:00	0:00:00
Last Month	N/A	N/A	0	0	0:00:00	0:00:00

The following table describes the fields in this screen.

**Table 149** Call History > Summary

LABEL	DESCRIPTION
Type of Summary	This field displays the time period for which the entry applies.
Start Time	This field displays the start time of the first incoming or outgoing call in the time period.
End Time	This field displays the end time of the last incoming or outgoing call in the time period.
Tx Packets	This field displays the total number of packets transmitted within this time period.
Rs Packets	This field displays the total number of packets received within this time period.
Duration of PSTN	This field displays the total time spent on all incoming and outgoing PSTN calls within this time period.
Duration of VoIP	This field displays total time spent on all incoming and outgoing VoIP calls within this time period.

## 26.3 Viewing Call History

Use the **Call History** screen to see records of incoming and outgoing PSTN/ISDN and VoIP calls. The information includes duration of phone calls, the packet statistics, local identity (the number of the phone connected to the ZyXEL Device) and the peer number associated with each call.

Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.



The ZyXEL Device records up to 150 phone calls and clears old records after it fills.

Click **Maintenance > Call History > Call History**. The following screen displays.

**Figure 228** Call History > Call History

Summary	Call History	Call History Settings						
<b>View Call History</b>								
View Call History	All Call History	Email Log Now Refresh Clear Call History						
Next Page:	1							
#	Type	Time ▲	Duration	Local Identity	Peer Number	TxPacket	RxPacket	Interface
1	Missed Call	01/01/2000 16:07:06	0:00:00	55002	22001	0	0	SIP
2	Dialed Call	01/01/2000 16:05:54	0:00:13	Phone 1	0168	0	0	PSTN
3	Received Call	01/01/2000 15:50:23	0:00:02	23	**11	0	0	ISDN
4	Received Call	01/01/2000 15:47:27	0:00:06	22	**11	0	0	ISDN
5	Dialed Call	01/01/2000 15:35:35	0:00:09	23	**11	0	0	ISDN
6	Received Call	01/01/2000 15:34:06	0:00:00	55002	22001	0	0	SIP
7	Received Call	01/01/2000 15:33:37	0:00:00	55002	22001	0	0	SIP

The following table describes the fields in this screen.

**Table 150** Call History > Call History

LABEL	DESCRIPTION
View Call History	Select the type of call you want to view <ul style="list-style-type: none"> <li>• All Call History</li> <li>• Missed Calls</li> <li>• Dialed Calls</li> <li>• Received Calls</li> </ul> Select <b>All Call History</b> to view the call history of all types of calls Select <b>Missed Calls</b> to view the history of the incoming calls you did not pick up. Select <b>Dialed Calls</b> to view the history of the outgoing calls you made. Select <b>Received Calls</b> to view the history of the incoming calls you picked up.
Email Log Now	Click this to send the call history to the e-mail address specified in the <b>Call History Settings</b> screen (make sure that you have first filled in the <b>E-mail Call History Settings</b> fields in the <b>Call History Settings</b> screen).
Refresh	Click <b>Refresh</b> to renew the screen.
Clear Call History	Click <b>Clear Call History</b> to delete all call history records.
Next page	Select the page you want to view.
#	This field is a sequential value and is not associated with a specific entry.
Type	This field displays the type of call you select in the <b>View Call History</b> field.
Time	This field displays the time this phone call was made.
Duration	This field displays the time you spent on this phone call.
Local Identity	This field displays the number you configured on the ZyXEL Device's phone port used in this phone call.
Peer Number	This field displays the phone number of the party associated with this phone call.
Tx Packets	This field displays the number of packets transmitted during this phone call.
Rs Packets	This field displays the number of packets received during this phone call.
Interface	This field displays the interface used to make this phone call.

## 26.4 Configuring Call History Settings

Use the **Call History Settings** screen to configure where the ZyXEL Device is to send call history records, and the schedule for saving and sending the records.

To change your ZyXEL Device's call history settings, click **Maintenance > Call History > Call History Settings**. The screen appears as follows.

**Figure 229** Call History > Call History Settings

The screenshot shows the 'Call History Settings' configuration page. It has three main sections: 'E-mail Call History Settings', 'Save Call History Settings', and 'Summary of Call History Settings'.  
**E-mail Call History Settings:** This section allows configuring email parameters for sending call history. It includes fields for 'Mail Server' (Outgoing SMTP Server Name or IP Address), 'Mail Subject', 'Send Call History to' (E-Mail Address), and options for 'Enable SMTP Authentication' (User Name and Password). It also defines a 'Send Call History Schedule' (When Log is Full) and specific days and times for sending.  
**Save Call History Settings:** This section defines a scheduled save of call history. It includes a 'Save Call History Schedule' (Hourly), a 'Day for Saving Call History' (Sunday), and a 'Time for Saving Call History' (00:00).  
**Summary of Call History Settings:** This section specifies the start day of every month for saving call history, indicated by a dropdown menu set to '0'. At the bottom are 'Apply' and 'Cancel' buttons.

The following table describes the fields in this screen.

**Table 151** Call History > Call History Settings

LABEL	DESCRIPTION
<b>E-mail Call History Settings</b>	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, call history records will not be sent.
Mail Subject	Type a title that you want to be in the subject line of the call history e-mail messages the ZyXEL Device sends.
Send Call History to	The ZyXEL Device sends call history records to the e-mail address specified in this field. If this field is left blank, the ZyXEL Device does not send logs via e-mail.
Enable SMTP Authentication	SMTP (Simple Mail Transfer Protocol) is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. Select this to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive call history e-mails.
User Name	Enter the user name (up to 31 characters) (usually the user name of a mail account).
Password	Enter the password associated with the user name above.
Send Call History Schedule	<p>This field is used to configure the frequency of call history records being sent as e-mail:</p> <ul style="list-style-type: none"> <li>• When Log is Full</li> <li>• Hourly</li> <li>• Daily</li> <li>• Weekly</li> <li>• None</li> </ul> <p>If you select <b>Weekly</b> or <b>Daily</b>, specify a time of day when the e-mail should be sent. If you select <b>Weekly</b>, then also specify which day of the week the e-mail should be sent. If you select <b>When Log is Full</b>, an alert is sent when the call history fills up. If you select <b>None</b>, no call history records are sent.</p>
Day for Sending Call History	Select which day of the week to send the call history records.
Time for Sending Call History	Enter the time of the day in 24-hour format (for example, “23:00” is 11:00 pm) to send the call history records.
Clear Sending Call History after sending mail	Select this to delete all the call history records after they have been e-mailed.
<b>Save Call History Settings</b>	
Save Call History Schedule	<p>This field is used to configure the frequency of call history records being saved on the ZyXEL Device:</p> <ul style="list-style-type: none"> <li>• Hourly</li> <li>• Daily</li> <li>• Weekly</li> </ul> <p>If you select <b>Weekly</b> or <b>Daily</b>, specify a time of day when the e-mail should be sent. If you select <b>Weekly</b>, then also specify which day of the week the e-mail should be sent.</p>
Time for Saving Call History	Enter the time of the day in 24-hour format (for example, 23:00 is 11:00 pm) to save the call history records.
<b>Summary of Call History Settings</b>	
Start Day of Every Month	<p>Enter the date you want the ZyXEL Device starts to record call history of all phone calls every month.</p> <p>For example, enter “5” as the start date of every month. You have a list of phone call records of one single month from 5th of the current month till 4th of next month.</p>

**Table 151** Call History > Call History Settings

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to return to the previously saved settings.

# Logs

This chapter contains information about configuring general log settings and viewing the ZyXEL Device's logs.

## 27.1 Logs Overview

The web configurator allows you to choose which categories of events and/or alerts to have the ZyXEL Device log and then display the logs or have the ZyXEL Device send them to an administrator (as e-mail) or to a syslog server.

### 27.1.1 Alerts and Logs

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

## 27.2 Viewing the Logs

Click **Maintenance > Logs** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see [Section 27.3 on page 388](#)).

Log entries in red indicate alerts. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

**Figure 230** View Log

View Logs					
Display:		Email Log Now		Refresh	Clear Log
#	Time ▲	Message	Source	Destination	Notes
1	01/01/2000 00:33:40	WEB Login Successfully			User:admin
2	01/01/2000 00:31:32	none: UDP	192.168.1.1:53	192.168.1.34:1197	ACCESS PERMITTED
3	01/01/2000 00:31:32	none: UDP	192.168.1.1:53	192.168.1.34:1196	ACCESS PERMITTED
4	01/01/2000 00:31:32	none: UDP	192.168.1.1:53	192.168.1.34:1195	ACCESS PERMITTED
5	01/01/2000 00:30:23	WEB Login Successfully			User:user

The following table describes the fields in this screen.

**Table 152** View Log

LABEL	DESCRIPTION
Display	The categories that you select in the <b>Log Settings</b> screen display in the drop-down list box. Select a category of logs to view; select <b>All Logs</b> to view logs from all of the log categories that you selected in the <b>Log Settings</b> page.
Email Log Now	Click <b>Email Log Now</b> to send the log screen to the e-mail address specified in the <b>Log Settings</b> page (make sure that you have first filled in the <b>E-mail Log Settings</b> fields in <b>Log Settings</b> ).
Refresh	Click <b>Refresh</b> to renew the log screen.
Clear Log	Click <b>Clear Log</b> to delete all the logs.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Notes	This field displays additional information about the log entry.

## 27.3 Configuring Log Settings

Use the **Log Settings** screen to configure to where the ZyXEL Device is to send logs; the schedule for when the ZyXEL Device is to send the logs and which logs and/or immediate alerts the ZyXEL Device is to record. See [Section 27.1 on page 387](#) for more information.

To change your ZyXEL Device's log settings, click **Maintenance > Logs > Log Settings**. The screen appears as shown.

Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full. Selecting many alert and/or log categories (especially **Access Control**) may result in many emails being sent.

**Figure 231** Log Settings

The screenshot shows the 'Log Settings' page with the following sections:

- E-mail Log Settings:**
  - Mail Server: [Text Box] (Outgoing SMTP Server Name or IP Address)
  - Mail Subject: [Text Box]
  - Send Log to: [Text Box] (E-Mail Address)
  - Send Alerts to: [Text Box] (E-Mail Address)
  - Enable SMTP Authentication
    - User Name: [Text Box]
    - Password: [Text Box]
  - Log Schedule: [Select Box] (None, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday)
    - Day for Sending Log: [Select Box] (Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday)
    - Time for Sending Log: [Text Box] (hour) [Text Box] (minute)
  - Clear log after sending mail
- Syslog Logging:**
  - Active
  - Syslog IP Address: [Text Box] (Server Name or IP Address) 0.0.0.0
  - Log Facility: [Select Box] (Local 1)
- Active Log and Alert:**

<b>Log</b>	<b>Send Immediate Alert</b>
<input checked="" type="checkbox"/> System Maintenance	<input type="checkbox"/> System Errors
<input checked="" type="checkbox"/> System Errors	<input type="checkbox"/> Access Control
<input checked="" type="checkbox"/> Access Control	<input type="checkbox"/> Blocked Web Sites
<input checked="" type="checkbox"/> UPnP	<input type="checkbox"/> Attacks
<input checked="" type="checkbox"/> Forward Web Sites	<input type="checkbox"/> IPSec
<input checked="" type="checkbox"/> Blocked Web Sites	<input type="checkbox"/> IKE
<input checked="" type="checkbox"/> Attacks	<input type="checkbox"/> PKI
<input type="checkbox"/> IPSec	
<input checked="" type="checkbox"/> IKE	
<input checked="" type="checkbox"/> Any IP	
<input type="checkbox"/> PKI	
<input checked="" type="checkbox"/> 802.1x	
<input checked="" type="checkbox"/> SIP	
<input checked="" type="checkbox"/> RTP	
<input checked="" type="checkbox"/> FSM	

Buttons at the bottom: Apply, Cancel.

The following table describes the fields in this screen.

**Table 153** Log Settings

LABEL	DESCRIPTION
<b>E-mail Log Settings</b>	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via E-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the ZyXEL Device sends. Not all ZyXEL Device models have this field.
Send Log to	The ZyXEL Device sends logs to the e-mail address specified in this field. If this field is left blank, the ZyXEL Device does not send logs via e-mail.

**Table 153** Log Settings

LABEL	DESCRIPTION
Send Alerts to	Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the E-mail address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via E-mail.
Enable SMTP Authentication	SMTP (Simple Mail Transfer Protocol) is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the e-mail logs.
User Name	Enter the user name (up to 31 characters) (usually the user name of a mail account).
Password	Enter the password associated with the user name above.
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: <ul style="list-style-type: none"> <li>• Daily</li> <li>• Weekly</li> <li>• Hourly</li> <li>• When Log is Full</li> <li>• None.</li> </ul> If you select <b>Weekly</b> or <b>Daily</b> , specify a time of day when the E-mail should be sent. If you select <b>Weekly</b> , then also specify which day of the week the E-mail should be sent. If you select <b>When Log is Full</b> , an alert is sent when the log fills up. If you select <b>None</b> , no log messages are sent.
Day for Sending Log	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Clear log after sending mail	Select the checkbox to delete all the logs after the ZyXEL Device sends an E-mail of the logs.
Syslog Logging	The ZyXEL Device sends a log to an external syslog server.
Active	Click <b>Active</b> to enable syslog logging.
Syslog IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the syslog server manual for more information.
Active Log and Alert	
Log	Select the categories of logs that you want to record.
Send Immediate Alert	Select log categories for which you want the ZyXEL Device to send E-mail alerts immediately.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to return to the previously saved settings.

## 27.4 SMTP Error Messages

If there are difficulties in sending e-mail the following error message appears.

"SMTP action request failed. ret= ??". The "???" are described in the following table.

**Table 154** SMTP Error Messages

-1 means ZyXEL Device out of socket
-2 means tcp SYN fail
-3 means smtp server OK fail
-4 means HELO fail
-5 means MAIL FROM fail
-6 means RCPT TO fail
-7 means DATA fail
-8 means mail data send fail

### 27.4.1 Example E-mail Log

An "End of Log" message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.

- You may edit the subject title.
- The date format here is Day-Month-Year.
- The date format here is Month-Day-Year. The time format is Hour-Minute-Second.
- "End of Log" message shows that a complete log has been sent.

**Figure 232** E-mail Log Example

```

Subject: Firewall Alert From
Date: Fri, 07 Apr 2000 10:05:42
From: user@zyxel.com
To: user@zyxel.com
1|Apr 7 00 |From:192.168.1.1      To:192.168.1.255 |default policy |forward
| 09:54:03 |UDP      src port:00520 dest port:00520 |<1,00>   |
2|Apr 7 00 |From:192.168.1.131    To:192.168.1.255 |default policy |forward
| 09:54:17 |UDP      src port:00520 dest port:00520 |<1,00>   |
3|Apr 7 00 |From:192.168.1.6      To:10.10.10.10 |match       |forward
| 09:54:19 |UDP      src port:03516 dest port:00053 |<1,01>   |
.....{snip}.....
.....{snip}.....
126|Apr 7 00 |From:192.168.1.1      To:192.168.1.255 |match       |forward
| 10:05:00 |UDP      src port:00520 dest port:00520 |<1,02>   |
127|Apr 7 00 |From:192.168.1.131    To:192.168.1.255 |match       |forward
| 10:05:17 |UDP      src port:00520 dest port:00520 |<1,02>   |
128|Apr 7 00 |From:192.168.1.1      To:192.168.1.255 |match       |forward
| 10:05:30 |UDP      src port:00520 dest port:00520 |<1,02>   |
End of Firewall Log

```

## 27.5 Log Descriptions

This section provides descriptions of example log messages.

**Table 155** System Maintenance Logs

LOG MESSAGE	DESCRIPTION
Time calibration is successful	The router has adjusted its time based on information from the time server.
Time calibration failed	The router failed to get information from the time server.
WAN interface gets IP: %s	A WAN interface got a new IP address from the DHCP, PPPoE, PPTP or dial-up server.
DHCP client IP expired	A DHCP client's IP address has expired.
DHCP server assigns %s	The DHCP server assigned an IP address to a client.
Successful WEB login	Someone has logged on to the router's web configurator interface.
WEB login failed	Someone has failed to log on to the router's web configurator interface.
Successful TELNET login	Someone has logged on to the router via telnet.
TELNET login failed	Someone has failed to log on to the router via telnet.
Successful FTP login	Someone has logged on to the router via ftp.
FTP login failed	Someone has failed to log on to the router via ftp.
NAT Session Table is Full!	The maximum number of NAT session table entries has been exceeded and the table is full.
Starting Connectivity Monitor	Starting Connectivity Monitor.
Time initialized by Daytime Server	The router got the time and date from the Daytime server.
Time initialized by Time server	The router got the time and date from the time server.
Time initialized by NTP server	The router got the time and date from the NTP server.
Connect to Daytime server fail	The router was not able to connect to the Daytime server.
Connect to Time server fail	The router was not able to connect to the Time server.
Connect to NTP server fail	The router was not able to connect to the NTP server.
Too large ICMP packet has been dropped	The router dropped an ICMP packet that was too large.
Configuration Change: PC = 0x% Task ID = 0x% x	The router is saving configuration changes.
Successful SSH login	Someone has logged on to the router's SSH server.
SSH login failed	Someone has failed to log on to the router's SSH server.
Successful HTTPS login	Someone has logged on to the router's web configurator interface using HTTPS protocol.
HTTPS login failed	Someone has failed to log on to the router's web configurator interface using HTTPS protocol.

**Table 156** System Error Logs

LOG MESSAGE	DESCRIPTION
%s exceeds the max. number of session per host!	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.
setNetBIOSFilter: calloc error	The router failed to allocate memory for the NetBIOS filter settings.
readNetBIOSFilter: calloc error	The router failed to allocate memory for the NetBIOS filter settings.
WAN connection is down.	A WAN connection is down. You cannot access the network through this interface.

**Table 157** Access Control Logs

LOG MESSAGE	DESCRIPTION
Firewall default policy: [ TCP   UDP   IGMP   ESP   GRE   OSPF ] <Packet Direction>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched the default policy and was blocked or forwarded according to the default policy's setting.
Firewall rule [NOT] match:[ TCP   UDP   IGMP   ESP   GRE   OSPF ] <Packet Direction>, <rule:%d>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched (or did not match) a configured firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
Triangle route packet forwarded: [ TCP   UDP   IGMP   ESP   GRE   OSPF ]	The firewall allowed a triangle route session to pass through.
Packet without a NAT table entry blocked: [ TCP   UDP   IGMP   ESP   GRE   OSPF ]	The router blocked a packet that didn't have a corresponding NAT table entry.
Router sent blocked web site message: TCP	The router sent a message to notify a user that the router blocked access to a web site that the user requested.

**Table 158** TCP Reset Logs

LOG MESSAGE	DESCRIPTION
Under SYN flood attack, sent TCP RST	The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.)
Exceed TCP MAX incomplete, sent TCP RST	The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.) Note: Refer to <b>TCP Maximum Incomplete</b> in the <b>Firewall Attack Alerts</b> screen.
Peer TCP state out of order, sent TCP RST	The router sent a TCP reset packet when a TCP connection state was out of order. Note: The firewall refers to RFC793 Figure 6 to check the TCP state.
Firewall session time out, sent TCP RST	The router sent a TCP reset packet when a dynamic firewall session timed out. Default timeout values: ICMP idle timeout (s): 60 UDP idle timeout (s): 60 TCP connection (three way handshaking) timeout (s): 30 TCP FIN-wait timeout (s): 60 TCP idle (established) timeout (s): 3600

**Table 158** TCP Reset Logs (continued)

LOG MESSAGE	DESCRIPTION
Exceed MAX incomplete, sent TCP RST	The router sent a TCP reset packet when the number of incomplete connections (TCP and UDP) exceeded the user-configured threshold. (Incomplete count is for all TCP and UDP connections through the firewall.) Note: When the number of incomplete connections (TCP + UDP) > "Maximum Incomplete High", the router sends TCP RST packets for TCP connections and destroys TOS (firewall dynamic sessions) until incomplete connections < "Maximum Incomplete Low".
Access block, sent TCP RST	The router sends a TCP RST packet and generates this log if you turn on the firewall TCP reset mechanism (via CLI command: "sys firewall tcprst").

**Table 159** Packet Filter Logs

LOG MESSAGE	DESCRIPTION
[ TCP   UDP   ICMP   IGMP   Generic ] packet filter matched (set: %d, rule: %d)	Attempted access matched a configured filter rule (denoted by its set and rule number) and was blocked or forwarded according to the rule.

For type and code details, see [Table 168 on page 397](#).

**Table 160** ICMP Logs

LOG MESSAGE	DESCRIPTION
Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>	ICMP access matched the default policy and was blocked or forwarded according to the user's setting.
Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>	ICMP access matched (or didn't match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
Triangle route packet forwarded: ICMP	The firewall allowed a triangle route session to pass through.
Packet without a NAT table entry blocked: ICMP	The router blocked a packet that didn't have a corresponding NAT table entry.
Unsupported/out-of-order ICMP: ICMP	The firewall does not support this kind of ICMP packets or the ICMP packets are out of order.
Router reply ICMP packet: ICMP	The router sent an ICMP reply packet to the sender.

**Table 161** CDR Logs

LOG MESSAGE	DESCRIPTION
board %d line %d channel %d, call %d, %s C01 Outgoing Call dev=%x ch=%x %s	The router received the setup requirements for a call. "call" is the reference (count) number of the call. "dev" is the device type (3 is for dial-up, 6 is for PPPoE, 10 is for PPTP). "channel" or "ch" is the call channel ID. For example, "board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0" Means the router has dialed to the PPPoE server 3 times.

**Table 161** CDR Logs (continued)

LOG MESSAGE	DESCRIPTION
board %d line %d channel %d, call %d, %s C02 OutCall Connected %d %s	The PPPoE, PPTP or dial-up call is connected.
board %d line %d channel %d, call %d, %s C02 Call Terminated	The PPPoE, PPTP or dial-up call was disconnected.

**Table 162** PPP Logs

LOG MESSAGE	DESCRIPTION
ppp:LCP Starting	The PPP connection's Link Control Protocol stage has started.
ppp:LCP Opening	The PPP connection's Link Control Protocol stage is opening.
ppp:CHAP Opening	The PPP connection's Challenge Handshake Authentication Protocol stage is opening.
ppp:IPCP Starting	The PPP connection's Internet Protocol Control Protocol stage is starting.
ppp:IPCP Opening	The PPP connection's Internet Protocol Control Protocol stage is opening.
ppp:LCP Closing	The PPP connection's Link Control Protocol stage is closing.
ppp:IPCP Closing	The PPP connection's Internet Protocol Control Protocol stage is closing.

**Table 163** UPnP Logs

LOG MESSAGE	DESCRIPTION
UPnP pass through Firewall	UPnP packets can pass through the firewall.

**Table 164** Content Filtering Logs

LOG MESSAGE	DESCRIPTION
%s: block keyword	The content of a requested web page matched a user defined keyword.
%s	The system forwarded web content.

For type and code details, see [Table 168 on page 397](#).

**Table 165** Attack Logs

LOG MESSAGE	DESCRIPTION
attack [ TCP   UDP   IGMP   ESP   GRE   OSPF ]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF attack.
attack ICMP (type:%d, code:%d)	The firewall detected an ICMP attack.
land [ TCP   UDP   IGMP   ESP   GRE   OSPF ]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF land attack.
land ICMP (type:%d, code:%d)	The firewall detected an ICMP land attack.

**Table 165** Attack Logs (continued)

LOG MESSAGE	DESCRIPTION
ip spoofing - WAN [ TCP   UDP   IGMP   ESP   GRE   OSPF ]	The firewall detected an IP spoofing attack on the WAN port.
ip spoofing - WAN ICMP (type:%d, code:%d)	The firewall detected an ICMP IP spoofing attack on the WAN port.
icmp echo : ICMP (type:%d, code:%d)	The firewall detected an ICMP echo attack.
syn flood TCP	The firewall detected a TCP syn flood attack.
ports scan TCP	The firewall detected a TCP port scan attack.
teardrop TCP	The firewall detected a TCP teardrop attack.
teardrop UDP	The firewall detected an UDP teardrop attack.
teardrop ICMP (type:%d, code:%d)	The firewall detected an ICMP teardrop attack.
illegal command TCP	The firewall detected a TCP illegal command attack.
NetBIOS TCP	The firewall detected a TCP NetBIOS attack.
ip spoofing - no routing entry [ TCP   UDP   IGMP   ESP   GRE   OSPF ]	The firewall classified a packet with no source routing entry as an IP spoofing attack.
ip spoofing - no routing entry ICMP (type:%d, code:%d)	The firewall classified an ICMP packet with no source routing entry as an IP spoofing attack.
vulnerability ICMP (type:%d, code:%d)	The firewall detected an ICMP vulnerability attack.
traceroute ICMP (type:%d, code:%d)	The firewall detected an ICMP traceroute attack.

**Table 166** 802.1X Logs

LOG MESSAGE	DESCRIPTION
Local User Database accepts user.	A user was authenticated by the local user database.
Local User Database reports user credential error.	A user was not authenticated by the local user database because of an incorrect user password.
Local User Database does not find user's credential.	A user was not authenticated by the local user database because the user is not listed in the local user database.
RADIUS accepts user.	A user was authenticated by the RADIUS Server.
RADIUS rejects user. Pls check RADIUS Server.	A user was not authenticated by the RADIUS Server. Please check the RADIUS Server.
Local User Database does not support authentication method.	The local user database only supports the EAP-MD5 method. A user tried to use another authentication method and was not authenticated.
User logout because of session timeout expired.	The router logged out a user whose session expired.
User logout because of user deassociation.	The router logged out a user who ended the session.

**Table 166** 802.1X Logs (continued)

LOG MESSAGE	DESCRIPTION
User logout because of no authentication response from user.	The router logged out a user from which there was no authentication response.
User logout because of idle timeout expired.	The router logged out a user whose idle timeout period expired.
User logout because of user request.	A user logged out.
Local User Database does not support authentication method.	A user tried to use an authentication method that the local user database does not support (it only supports EAP-MD5).
No response from RADIUS. Pls check RADIUS Server.	There is no response message from the RADIUS server, please check the RADIUS server.
Use Local User Database to authenticate user.	The local user database is operating as the authentication server.
Use RADIUS to authenticate user.	The RADIUS server is operating as the authentication server.
No Server to authenticate user.	There is no authentication server to authenticate a user.
Local User Database does not find user's credential.	A user was not authenticated by the local user database because the user is not listed in the local user database.

**Table 167** ACL Setting Notes

PACKET DIRECTION	DIRECTION	DESCRIPTION
(L to W)	LAN to WAN	ACL set for packets traveling from the LAN to the WAN.
(W to L)	WAN to LAN	ACL set for packets traveling from the WAN to the LAN.
(L to L/ZyXEL Device)	LAN to LAN/ZyXEL Device	ACL set for packets traveling from the LAN to the LAN or the ZyXEL Device.
(W to W/ZyXEL Device)	WAN to WAN/ZyXEL Device	ACL set for packets traveling from the WAN to the WAN or the ZyXEL Device.

**Table 168** ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench

**Table 168** ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

**Table 169** Syslog Logs

LOG MESSAGE	DESCRIPTION
<Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address last three numbers>" cat="<category>"	"This message is sent by the system ("RAS" displays as the system name if you haven't configured one) when the router generates a syslog. The facility is defined in the web MAIN MENU->LOGS->Log Settings page. The severity is the log's syslog class. The definition of messages and notes are defined in the various log charts throughout this appendix. The "devID" is the last three characters of the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs.

**Table 170** SIP Logs

LOG MESSAGE	DESCRIPTION
SIP Registration Success by SIP:SIP Phone Number	The listed SIP account was successfully registered with a SIP register server.
SIP Registration Fail by SIP:SIP Phone Number	An attempt to register the listed SIP account with a SIP register server was not successful.

**Table 170** SIP Logs (continued)

LOG MESSAGE	DESCRIPTION
SIP UnRegistration Success by SIP:SIP Phone Number	The listed SIP account's registration was deleted from the SIP register server.
SIP UnRegistration Fail by SIP:SIP Phone Number	An attempt to delete the listed SIP account's registration from the SIP register server failed.

**Table 171** RTP Logs

LOG MESSAGE	DESCRIPTION
Error, RTP init fail	The initialization of an RTP session failed.
Error, Call fail: RTP connect fail	A VoIP phone call failed because the RTP session could not be established.
Error, RTP connection cannot close	The termination of an RTP session failed.

**Table 172** FSM Logs: Caller Side

LOG MESSAGE	DESCRIPTION
VoIP Call Start Ph[Phone Port Number] <- Outgoing Call Number	Someone used a phone connected to the listed phone port to initiate a VoIP call to the listed destination.
VoIP Call Established Ph[Phone Port] -> Outgoing Call Number	Someone used a phone connected to the listed phone port to make a VoIP call to the listed destination.
VoIP Call End Phone [Phone Port]	A VoIP phone call made from a phone connected to the listed phone port has terminated.

**Table 173** FSM Logs: Callee Side

LOG MESSAGE	DESCRIPTION
VoIP Call Start from SIP[SIP Port Number]	A VoIP phone call came to the ZyXEL Device from the listed SIP number.
VoIP Call Established Ph[Phone Port] <- Outgoing Call Number	A VoIP phone call was set up from the listed SIP number to the ZyXEL Device.
VoIP Call End Phone [Phone Port]	A VoIP phone call that came into the ZyXEL Device has terminated.

**Table 174** PSTN Logs

LOG MESSAGE	DESCRIPTION
PSTN Call Start	A PSTN call has been initiated.
PSTN Call End	A PSTN call has terminated.
PSTN Call Established	A PSTN call has been set up.

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to RFC 2408 for detailed information on each type.

**Table 175** RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash
SIG	Signature
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

# Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- ZyXEL Device Access and Login
- Internet Access
- Phone Calls and VoIP

## 28.1 Power, Hardware Connections, and LEDs



---

The ZyXEL Device does not turn on. None of the LEDs turn on.

---

- 1 Make sure the ZyXEL Device is turned on.
- 2 Make sure you are using the power adaptor or cord included with the ZyXEL Device.
- 3 Make sure the power adaptor or cord is connected to the ZyXEL Device and plugged in to an appropriate power source. Make sure the power source is turned on.
- 4 Turn the ZyXEL Device off and on.
- 5 If the problem continues, contact the vendor.



---

One of the LEDs does not behave as expected.

---

- 1 Make sure you understand the normal behavior of the LED. See [Section 1.5 on page 46](#).
- 2 Check the hardware connections. See the Quick Start Guide.
- 3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- 4 Turn the ZyXEL Device off and on.
- 5 If the problem continues, contact the vendor.

## 28.2 ZyXEL Device Access and Login



---

I forgot the IP address for the ZyXEL Device.

---

- 1 The default IP address is **192.168.1.1**.
- 2 If you changed the IP address and have forgotten it, you might get the IP address of the ZyXEL Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the ZyXEL Device (it depends on the network), so enter this IP address in your Internet browser.
- 3 If this does not work, you have to reset the device to its factory defaults. See [Section 1.6 on page 47](#).



---

I forgot the password.

---

- 1 The default password is **1234**.
- 2 If this does not work, you have to reset the device to its factory defaults. See [Section 1.6 on page 47](#).



---

I cannot see or access the **Login** screen in the web configurator.

---

- 1 Make sure you are using the correct IP address.
  - The default IP address is **192.168.1.1**.
  - If you changed the IP address ([Section 8.3.1 on page 118](#)), use the new IP address.
  - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I forgot the IP address for the ZyXEL Device](#).
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
- 3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See [Appendix B on page 447](#).
- 4 If you disabled **Any IP** ([Section 8.4.1 on page 123](#)), make sure your computer is in the same subnet as the ZyXEL Device. (If you know that there are routers between your computer and the ZyXEL Device, skip this step.)
  - If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See [Appendix A on page 435](#). Your ZyXEL Device is a DHCP server by default.
  - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the ZyXEL Device. See [Appendix A on page 435](#).

- 5 Reset the device to its factory defaults, and try to access the ZyXEL Device with the default IP address. See [Section 1.6 on page 47](#).
- 6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

#### Advanced Suggestions

- Try to access the ZyXEL Device using another service, such as Telnet. If you can access the ZyXEL Device, check the remote management settings and firewall rules to find out why the ZyXEL Device does not respond to HTTP.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to a **LAN/ETHERNET** port.



I can see the **Login** screen, but I cannot log in to the ZyXEL Device.

- 1 Make sure you have entered the user name and password correctly. The default password is **1234**. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 2 You cannot log in to the web configurator while someone is using Telnet to access the ZyXEL Device. Log out of the ZyXEL Device in the other session, or ask the person who is logged in to log out.
- 3 Turn the ZyXEL Device off and on.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 28.1 on page 401](#).



I cannot Telnet to the ZyXEL Device.

See the troubleshooting suggestions for [I cannot see or access the Login screen in the web configurator](#). Ignore the suggestions about your browser.



I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for [I cannot see or access the Login screen in the web configurator](#). Ignore the suggestions about your browser.

## 28.3 Internet Access



I cannot access the Internet.

---

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.5 on page 46](#).
- 2 Make sure you entered your ISP account information correctly in the wizard. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 3 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
- 4 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
- 5 If the problem continues, contact your ISP.



I cannot access the Internet anymore. I had access to the Internet (with the ZyXEL Device), but my Internet connection is not available anymore.

---

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.5 on page 46](#).
- 2 Turn the ZyXEL Device off and on.
- 3 If the problem continues, contact your ISP.



The Internet connection is slow or intermittent.

---

- 1 There might be a lot of traffic on the network. Look at the LEDs, and check [Section 1.5 on page 46](#). If the ZyXEL Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
- 2 Check the signal strength. If the signal strength is low, try moving the ZyXEL Device closer to the AP if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).
- 3 Turn the ZyXEL Device off and on.
- 4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

### Advanced Suggestions

- Check the settings for bandwidth management. If it is disabled, you might consider activating it. If it is enabled, you might consider changing the allocations.

- Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

## 28.4 Phone Calls and VoIP



The telephone port won't work or the telephone lacks a dial tone.

Check the telephone connections and telephone wire.

Make sure you have the **VoIP SIP Settings** screen properly configured.



I can access the Internet, but cannot make VoIP calls.

Make sure you have the **VoIP SIP Settings** screen properly configured.

One of the **PHONE** lights should come on. Make sure that your telephone is connected to the corresponding **PHONE** port.

You can also check the VoIP status in the **Status** screen.

If the VoIP settings are correct, use speed dial to make peer-to-peer calls. If you can make a call using speed dial, but not your SIP account, there may be something wrong with the SIP server - contact your VoIP service provider.



I cannot call from one of the ZyXEL Device's phone ports to the other phone port.

If you are using extension numbers to call from one phone to another, ensure that the **VoIP > Phone > Ext. Table** screen is correctly configured.

On a phone connected to one of the ZyXEL Device's **PHONE** ports, try pressing the pound key four times (###). This calls the phones connected to the other **PHONE** port.

If you are using a SIP account to call the other phone(s), make sure that both phone ports do not use the same SIP account. You cannot call the SIP number of the SIP account that you are using to make a call. The ZyXEL Device generates a busy tone and does not attempt to establish a call if the SIP number you dial matches the outgoing SIP number of the phone port you are using.

If you use different SIP accounts for each phone port, you can call from one to the other. For example, if you set **Phone 1** to use SIP account 1 and set **Phone 2** to use SIP account 2, then you can use **Phone 1** to call to SIP account 2's SIP number or **Phone 2** to call to SIP account 1's SIP number.



# Tools

This chapter explains how to upload new firmware, manage configuration files and restart your ZyXEL Device.



**Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE your ZyXEL Device.**

## 29.1 Introduction

Use the instructions in this chapter to change the device's configuration file or upgrade its firmware. After you configure your device, you can backup the configuration file to a computer. That way if you later misconfigure the device, you can upload the backed up configuration file to return to your previous settings. You can alternately upload the factory default configuration file if you want to return the device to the original default settings. The firmware determines the device's available features and functionality. You can download new firmware releases from your nearest ZyXEL FTP site (or [www.zyxel.com](http://www.zyxel.com)) to use to upgrade your device's performance.



**Only use firmware for your device's specific model. Refer to the label on the bottom of your ZyXEL Device.**

## 29.2 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. It arrives from ZyXEL with a "rom" filename extension. Once you have customized the ZyXEL Device's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the “ras” file) is the system firmware and has a “bin” filename extension. Find this firmware at [www.zyxel.com](http://www.zyxel.com). With many FTP and TFTP clients, the filenames are similar to those seen next.

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the ZyXEL Device.

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to the computer file "config.cfg".

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the ZyXEL Device only recognizes “rom-0” and “ras”. Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the ZyXEL Device and the external filename refers to the filename not on the ZyXEL Device, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, see the **Status** screen to confirm that you have uploaded the correct firmware version.

**Table 176** Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	This is the configuration filename on the ZyXEL Device. Uploading the rom-0 file replaces the entire ROM file system, including your ZyXEL Device configurations, system-related data (including the default password), the error log and the trace log.	*.rom
Firmware	Ras	This is the generic name for the ZyNOS firmware on the ZyXEL Device.	*.bin

## 29.3 File Maintenance Over WAN

TFTP, FTP and Telnet over the WAN will not work when:

- 1 The firewall is active (turn the firewall off or create a firewall rule to allow access from the WAN).
- 2 You have disabled Telnet service in menu 24.11.
- 3 You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Telnet service.
- 4 The IP you entered in the **Secured Client IP** field in menu 24.11 does not match the client IP. If it does not match, the device will disconnect the Telnet session immediately.

## 29.4 Firmware Upgrade Screen

Click **Maintenance > Tools** to open the **Firmware** screen. Follow the instructions in this screen to upload firmware to your ZyXEL Device. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See [Section 29.9 on page 416](#) for upgrading firmware using FTP/TFTP commands.



**Do NOT turn off the ZyXEL Device while firmware upload is in progress!**

**Figure 233** Firmware Upgrade

To upgrade the internal device firmware, browse to the location of the binary (.BIN) upgrade file and click **Upload**. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure

Current Firmware Version: V3.40(ADV.2)b2 | 10/27/2006

File Path:

.....

The following table describes the labels in this screen.

**Table 177** Firmware Upgrade

LABEL	DESCRIPTION
Current Firmware Version	This is the present Firmware version and the date created.
File Path	Type in the location of the file you want to upload in this field or click <b>Browse ...</b> to find it.
Browse...	Click <b>Browse...</b> to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click <b>Upload</b> to begin the upload process. This process may take up to two minutes.

After you see the **Firmware Upload in Progress** screen, wait two minutes before logging into the ZyXEL Device again.

**Figure 234** Firmware Upload In Progress

The ZyXEL Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 235** Network Temporarily Disconnected

After two minutes, log in again and check your new firmware version in the **Status** screen.

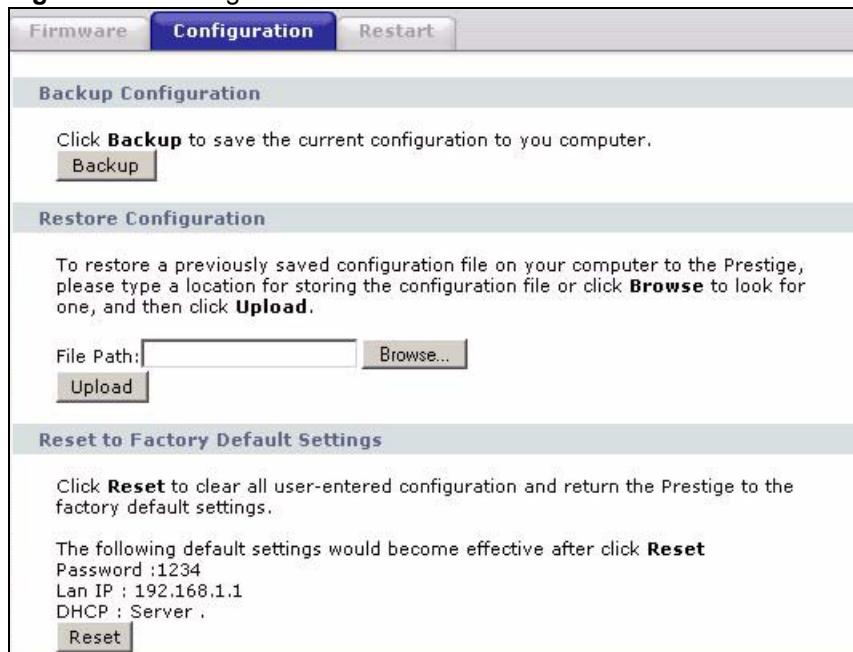
If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Firmware** screen.

**Figure 236** Error Message

## 29.5 Backup and Restore

See [Section 29.7 on page 413](#) and [Section 29.8 on page 416](#) for transferring configuration files using FTP/TFTP commands.

Click **Maintenance > Tools > Configuration**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

**Figure 237** Configuration

### 29.5.1 Backup Configuration

Backup Configuration allows you to back up (save) the ZyXEL Device's current configuration to a file on your computer. Once your ZyXEL Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the ZyXEL Device's current configuration to your computer.

### 29.5.2 Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your ZyXEL Device.

**Table 178** Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse ...</b> to find it.
Browse...	Click <b>Browse...</b> to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click <b>Upload</b> to begin the upload process.



Do not turn off the ZyXEL Device while configuration file upload is in progress.

After you see a “restore configuration successful” screen, you must then wait one minute before logging into the ZyXEL Device again.

**Figure 238** Configuration Upload Successful

The ZyXEL Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 239** Network Temporarily Disconnected

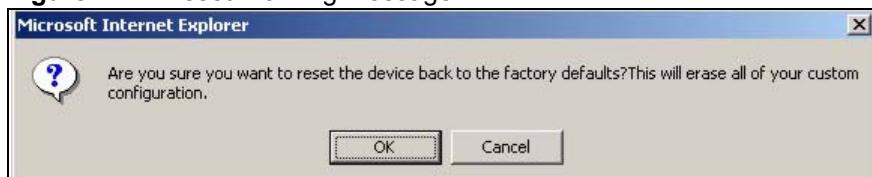
If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See [Appendix A on page 435](#) for details on how to set up your computer's IP address.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Configuration** screen.

**Figure 240** Configuration Upload Error

### 29.5.3 Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the ZyXEL Device to its factory defaults. The following warning screen appears.

**Figure 241** Reset Warning Message

**Figure 242** Reset In Process Message

You can also press the **RESET** button on the rear panel to reset the factory defaults of your ZyXEL Device. Refer to [Section 1.6 on page 47](#) for more information on the **RESET** button.

## 29.6 Restart

System restart allows you to reboot the ZyXEL Device without turning the power off.

Click **Maintenance > Tools > Restart**. Click **Restart** to have the ZyXEL Device reboot. This does not affect the ZyXEL Device's configuration.

**Figure 243** Restart Screen

## 29.7 Using FTP or TFTP to Back Up Configuration

This section covers how to use FTP or TFTP to save your device's configuration file to your computer.

### 29.7.1 Using the FTP Commands to Back Up Configuration

- 1 Launch the FTP client on your computer.
- 2 Enter “open”, followed by a space and the IP address of your ZyXEL Device.
- 3 Press [ENTER] when prompted for a username.
- 4 Enter your password as requested (the default is “1234”).
- 5 Enter “bin” to set transfer mode to binary.
- 6 Use “get” to transfer files from the ZyXEL Device to the computer, for example, “get rom-0 config.rom” transfers the configuration file on the ZyXEL Device to your

computer and renames it “config.rom”. See earlier in this chapter for more information on filename conventions.

- 7 Enter “quit” to exit the ftp prompt.

### 29.7.2 FTP Command Configuration Backup Example

This figure gives an example of using FTP commands from the DOS command prompt to save your device’s configuration onto your computer.

**Figure 244** FTP Session Example

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

### 29.7.3 Configuration Backup Using GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

**Table 179** General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

### 29.7.4 Backup Configuration Using TFTP

The ZyXEL Device supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next.

- 1** Use telnet from your computer to connect to the ZyXEL Device and log in. Because TFTP does not have any security checks, the ZyXEL Device records the IP address of the telnet client and accepts TFTP requests only from this address.
- 2** Enter command “sys stdio 0” to disable the management idle timeout, so the TFTP transfer will not be interrupted. Enter command “sys stdio 5” to restore the five-minute management idle timeout (default) when the file transfer is complete.
- 3** Launch the TFTP client on your computer and connect to the ZyXEL Device. Set the transfer mode to binary before starting data transfer.
- 4** Use the TFTP client (see the example below) to transfer files between the ZyXEL Device and the computer. The file name for the configuration file is “rom-0” (rom-zero, not capital o).

Note that the telnet connection must be active before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the ZyXEL Device to the computer and “binary” to set binary transfer mode.

### 29.7.5 TFTP Command Configuration Backup Example

The following is an example TFTP command:

```
tftp [-i] host get rom-0 config.rom
```

where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the ZyXEL Device IP address, “get” transfers the file source on the ZyXEL Device (rom-0, name of the configuration file on the ZyXEL Device) to the file destination on the computer and renames it config.rom.

### 29.7.6 Configuration Backup Using GUI-based TFTP Clients

The following table describes some of the fields that you may see in GUI-based TFTP clients.

**Table 180** General Commands for GUI-based TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the ZyXEL Device. 192.168.1.1 is the ZyXEL Device’s default IP address when shipped.
Send/Fetch	Use “Send” to upload the file to the ZyXEL Device and “Fetch” to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the ZyXEL Device. The filename for the firmware is “ras” and for the configuration file, is “rom-0”.
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

Refer to [Section 29.3 on page 408](#) to read about configurations that disallow TFTP and FTP over WAN.

## 29.8 Using FTP or TFTP to Restore Configuration

This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred method for restoring your current computer configuration to your device since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.



**Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE your device. When the Restore Configuration process is complete, the device automatically restarts.**

---

### 29.8.1 Restore Using FTP Session Example

**Figure 245** Restore Using FTP Session Example

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Refer to [Section 29.3 on page 408](#) to read about configurations that disallow TFTP and FTP over WAN.

## 29.9 FTP and TFTP Firmware and Configuration File Uploads

This section shows you how to upload firmware and configuration files.



**Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE your device.**

---

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client. The following sections give examples of how to upload the firmware and the configuration files.

### 29.9.1 FTP File Upload Command from the DOS Prompt Example

- 1 Launch the FTP client on your computer.
- 2 Enter “open”, followed by a space and the IP address of your device.
- 3 Press [ENTER] when prompted for a username.
- 4 Enter your password as requested (the default is “1234”).
- 5 Enter “bin” to set transfer mode to binary.
- 6 Use “put” to transfer files from the computer to the device, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the device and renames it “ras”. Similarly, “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the device and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the device to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.
- 7 Enter “quit” to exit the ftp prompt.

### 29.9.2 FTP Session Example of Firmware File Upload

**Figure 246** FTP Session Example of Firmware File Upload

```

331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit

```

More commands (found in GUI-based FTP clients) are listed earlier in this chapter.

Refer to [Section 29.3 on page 408](#) to read about configurations that disallow TFTP and FTP over WAN.

### 29.9.3 TFTP File Upload

The device also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next.

- 1 Use telnet from your computer to connect to the device and log in. Because TFTP does not have any security checks, the device records the IP address of the telnet client and accepts TFTP requests only from this address.

- 2** Enter the command “sys stdio 0” to disable the management idle timeout, so the TFTP transfer will not be interrupted. Enter “command sys stdio 5” to restore the five-minute management idle timeout (default) when the file transfer is complete.
- 3** Launch the TFTP client on your computer and connect to the device. Set the transfer mode to binary before starting data transfer.
- 4** Use the TFTP client (see the example below) to transfer files between the device and the computer. The file name for the firmware is “ras”.

Note that the telnet connection must be active and the device in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the device to the computer, “put” the other way around, and “binary” to set binary transfer mode.

#### 29.9.4 TFTP Upload Command Example

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

Where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the device’s IP address, “put” transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the device).

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

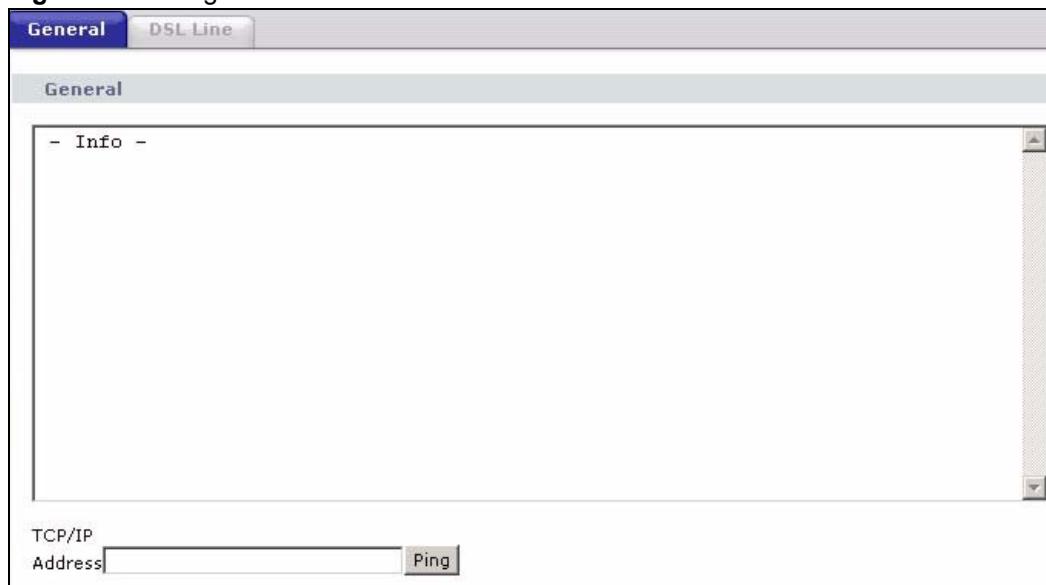
# Diagnostic

These read-only screens display information to help you identify problems with the ZyXEL Device.

## 30.1 General Diagnostic

Click **Maintenance > Diagnostic** to open the screen shown next.

**Figure 247** Diagnostic: General



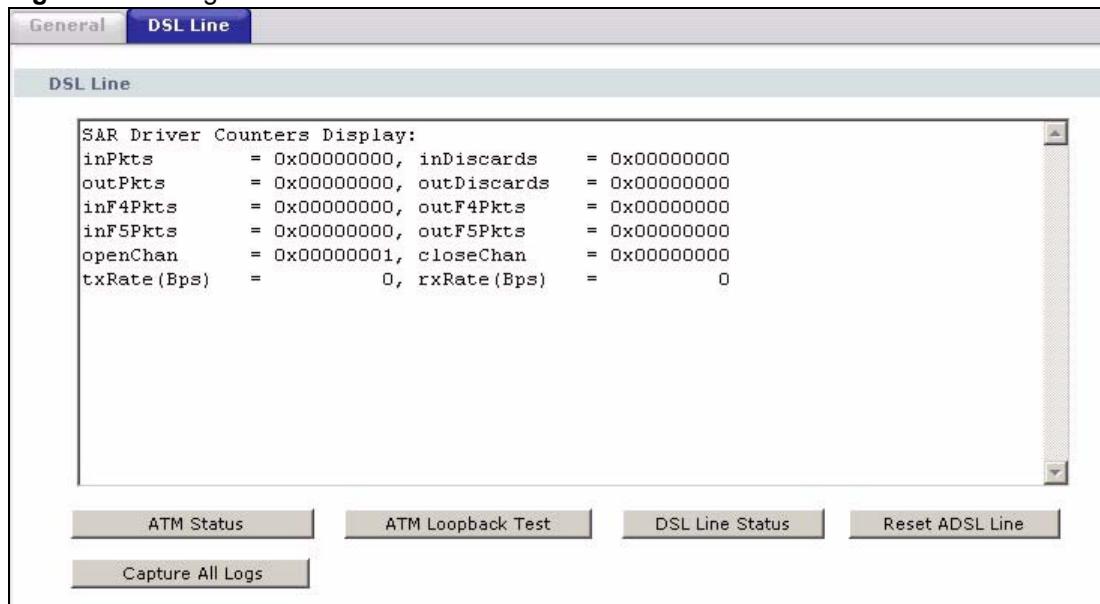
The following table describes the fields in this screen.

**Table 181** Diagnostic: General

LABEL	DESCRIPTION
TCP/IP Address	Type the IP address of a computer that you want to ping in order to test a connection.
Ping	Click this button to ping the IP address that you entered.

## 30.2 DSL Line Diagnostic

Click **Maintenance > Diagnostic > DSL Line** to open the screen shown next.

**Figure 248** Diagnostic: DSL Line

The following table describes the fields in this screen.

**Table 182** Diagnostic: DSL Line

LABEL	DESCRIPTION
ATM Status	<p>Click this button to view your DSL connection's Asynchronous Transfer Mode (ATM) statistics. ATM is a networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed.</p> <p>The (Segmentation and Reassembly) SAR driver translates packets into ATM cells. It also receives ATM cells and reassembles them into packets.</p> <p>These counters are set back to zero whenever the device starts up.</p> <p><b>inPkts</b> is the number of good ATM cells that have been received.</p> <p><b>inDiscards</b> is the number of received ATM cells that were rejected.</p> <p><b>outPkts</b> is the number of ATM cells that have been sent.</p> <p><b>outDiscards</b> is the number of ATM cells sent that were rejected.</p> <p><b>inF4Pkts</b> is the number of ATM Operations, Administration, and Management (OAM) F4 cells that have been received. See ITU recommendation I.610 for more on OAM for ATM.</p> <p><b>outF4Pkts</b> is the number of ATM OAM F4 cells that have been sent.</p> <p><b>inF5Pkts</b> is the number of ATM OAM F5 cells that have been received.</p> <p><b>outF5Pkts</b> is the number of ATM OAM F5 cells that have been sent.</p> <p><b>openChan</b> is the number of times that the ZyXEL Device has opened a logical DSL channel.</p> <p><b>closeChan</b> is the number of times that the ZyXEL Device has closed a logical DSL channel.</p> <p><b>txRate</b> is the number of bytes transmitted per second.</p> <p><b>rxRate</b> is the number of bytes received per second.</p>
ATM Loopback Test	Click this button to start the ATM loopback test. Make sure you have configured at least one PVC with proper VPIs/VCI before you begin this test. The ZyXEL Device sends an OAM F5 packet to the DSLAM/ATM switch and then returns it (loops it back) to the ZyXEL Device. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network.

**Table 182** Diagnostic: DSL Line (continued)

LABEL	DESCRIPTION
DSL Line Status	<p>Click this button to view statistics about the DSL connections.</p> <p><b>noise margin downstream</b> is the signal to noise ratio for the downstream part of the connection (coming into the ZyXEL Device from the ISP). It is measured in decibels. The higher the number the more signal and less noise there is.</p> <p><b>output power upstream</b> is the amount of power (in decibels) that the ZyXEL Device is using to transmit to the ISP.</p> <p><b>attenuation downstream</b> is the reduction in amplitude (in decibels) of the DSL signal coming into the ZyXEL Device from the ISP.</p> <p>Discrete Multi-Tone (DMT) modulation divides up a line's bandwidth into sub-carriers (sub-channels) of 4.3125 KHz each called tones. The rest of the display is the line's bit allocation. This is displayed as the number (in hexadecimal format) of bits transmitted for each tone. This can be used to determine the quality of the connection, whether a given sub-carrier loop has sufficient margins to support certain ADSL transmission rates, and possibly to determine whether particular specific types of interference or line attenuation exist. Refer to the ITU-T G.992.1 recommendation for more information on DMT.</p> <p>The better (or shorter) the line, the higher the number of bits transmitted for a DMT tone. The maximum number of bits that can be transmitted per DMT tone is 15. There will be some tones without any bits as there has to be space between the upstream and downstream channels.</p>
Reset ADSL Line	<p>Click this button to reinitialize the ADSL line. The large text box above then displays the progress and results of this operation, for example:</p> <p>"Start to reset ADSL Loading ADSL modem F/W... Reset ADSL Line Successfully!"</p>
Capture All Logs	<p>Click this button to display information and statistics about your ZyXEL Device's ATM statistics, DSL connection statistics, DHCP settings, firmware version, WAN and gateway IP address, VPI/VCI and LAN IP address.</p>



# Product Specifications

The following tables summarize the ZyXEL Device's hardware and firmware features.

## 31.1 Hardware Specifications

**Table 183** Hardware Specifications

SPECIFICATION	DESCRIPTION
Dimensions (W x D x H)	168 x 37 x 248 mm
Weight	390g
Power Specification	18VDC 1A
Built-in Switch	Four auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports
PHONE Ports	2 RJ-11 FXS POTS ports.
ISDN PHONE Port	1 RJ-45 FXS ISDN port
PSTN/ISDN Port	1 RJ-45 FXO PSTN or ISDN port
RESET Button	Restores factory defaults
Antenna	One attached external dipole antenna, 2dBi
Operating Environment	Temperature: 0° C ~ 40° C Humidity: 20% ~ 85% RH
Storage Environment	Temperature: -20° C ~ 60° C Humidity: 20% ~ 90% RH

## 31.2 Firmware Specifications

**Table 184** Firmware Specifications

Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
DHCP Server IP Pool	192.168.1.32 to 192.168.1.64
Static DHCP Addresses	10
Content Filtering	Web page blocking by URL keyword.
Static Routes	16 IP

**Table 184** Firmware Specifications (continued)

Device Management	Use the web configurator to easily configure the rich range of features on the ZyXEL Device.
Wireless Functionality	Allow the IEEE 802.11b and/or IEEE 802.11g wireless clients to connect to the ZyXEL Device wirelessly. Enable wireless security (WEP, WPA(2), WPA(2)-PSK) and/or MAC filtering to protect your wireless network.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator, an FTP or a TFTP tool to put it on the ZyXEL Device.  Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the ZyXEL Device's configuration. You can put it back on the ZyXEL Device later if you decide to revert back to an earlier configuration.
Network Address Translation (NAT)	Each computer on your network must have its own unique IP address. Use NAT to convert your public IP address(es) to multiple private IP addresses for the computers on your network.
Port Forwarding	If you have a server (mail or web server for example) on your network, you can use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the ZyXEL Device assign IP addresses, an IP default gateway and DNS servers to computers on your network.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.
IP Multicast	IP multicast is used to send traffic to a specific group of computers. The ZyXEL Device supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
Time and Date	Get the current time and date from an external server when you turn on your ZyXEL Device. You can also set the time manually. These dates and times are then used in logs.
Logs	Use logs for troubleshooting. You can send logs from the ZyXEL Device to an external syslog server.
Universal Plug and Play (UPnP)	A UPnP-enabled device can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.
Firewall	You can configure firewall on the ZyXEL Device for secure Internet access. When the firewall is on, by default, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files for example.
Content Filter	The ZyXEL Device blocks or allows access to web sites that you specify and blocks access to web sites with URLs that contain keywords that you specify. You can define time periods and days during which content filtering is enabled. You can also include or exclude particular computers on your network from content filtering.  You can also subscribe to category-based content filtering that allows your ZyXEL Device to check web sites against an external database.
Bandwidth Management	You can efficiently manage traffic on your network by reserving bandwidth and giving priority to certain types of traffic and/or to particular computers.
Remote Management	This allows you to decide whether a service (HTTP or FTP traffic for example) from a computer on a network (LAN or WAN for example) can access the ZyXEL Device.

**Table 184** Firmware Specifications (continued)

Zero Configuration Internet Access	Once you connect and turn on the device, it automatically detects the Internet connection settings (such as the VCI/VPI numbers and the encapsulation method) from the ISP and makes the necessary configuration changes. In cases where additional account information (such as an Internet account user name and password) is required or the ZyXEL Device cannot connect to the ISP, you will be redirected to web screen(s) for information input or troubleshooting.
Any IP	The Any IP feature allows a computer to access the Internet and the ZyXEL Device without changing the network settings (such as IP address and subnet mask) of the computer, when the IP addresses of the computer and the ZyXEL Device are not in the same subnet.
Auto Provisioning	Your VoIP service provider can automatically update your device's configuration via an auto-provisioning server.
IPSec VPN Capability	Establish a Virtual Private Network (VPN) to connect with business partners and branch offices using data encryption and the Internet to provide secure communications without the expense of leased site-to-site lines. The ZyXEL Device VPN is based on the IPSec standard and is interoperable with other IPSec-based VPN products. The ZyXEL Device supports up to two simultaneous IPSec connections.
Universal Plug and Play (UPnP)	Your device and other UPnP enabled devices can use the standard TCP/IP protocol to dynamically join a network, obtain an IP address and convey their capabilities to each other.
PPPoE Support (RFC2516)	PPPoE (Point-to-Point Protocol over Ethernet) emulates a dial-up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on your device is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers.
Other PPPoE Features	PPPoE idle time out PPPoE dial on demand
Multiple PVC (Permanent Virtual Circuits) Support	Your device supports up to 8 Permanent Virtual Circuits (PVCs).
IP Alias	IP alias allows you to partition a physical network into logical networks over the same Ethernet interface. Your device supports three logical LAN interfaces via its single physical Ethernet interface with the your device itself as the gateway for each LAN network.
IP Policy Routing (IPPR)	Traditionally, routing is based on the destination address only and the router takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator.
Packet Filters	Your device's packet filtering function allows added network security and management.

**Table 184** Firmware Specifications (continued)

ADSL Standards	Support ITU G.992.1 G.dmt (Annex B, U-R2) EOC specified in ITU-T G.992.1 ADSL2 G.dmt.bis (G.992.3) ADSL2 G-lite.bis (G.992.4) ADSL 2/2+ AnnexM ADSL2+ (G.992.5) Reach-Extended ADSL (RE ADSL) SRA (Seamless Rate Adaptation) Auto-negotiating rate adaptation ADSL physical connection ATM AAL5 (ATM Adaptation Layer type 5) Multi-protocol over AAL5 (RFC 2684/1483) PPP over ATM AAL5 (RFC 2364) PPP over Ethernet (RFC 2516) Multiple PPPoE VC-based and LLC-based multiplexing Up to 8 PVCs (Permanent Virtual Circuits) I.610 F4/F5 OAM Zero configuration
Other Protocol Support	PPP (Point-to-Point Protocol) link layer protocol Transparent bridging for unsupported network layer protocols RIP I/RIP II ICMP ATM QoS SNMP v1 and v2c with MIB II support (RFC 1213) IP Multicasting IGMP v1 and v2 IGMP Proxy
Management	Embedded Web Configurator CLI (Command Line Interpreter) SNMP v1 & v2c with MIB II Embedded FTP/TFTP Server for firmware upgrade and configuration file backup and restore Telnet for remote management Remote Management Control: Telnet, FTP, Web, SNMP and DNS. VoIP Auto-provisioning via TFTP / HTTP / HTTPS Remote Firmware Upgrade Syslog
Other Features	Zero Configuration (VC auto-hunting) Traffic Redirect Dynamic DNS SPTGEN QoS
Firewall	Stateful Packet Inspection Prevent Denial of Service attacks such as Ping of Death, SYN Flood, LAND, Smurf etc. Access Control of Service Content Filtering IP & Generic Packet Filtering Real time Attack Alerts and Logs Reports and logs SIP ALG passthrough

**Table 184** Firmware Specifications (continued)

NAT/SUA	Port Forwarding 1024 NAT sessions Multimedia application PPTP under NAT/SUA IPSec passthrough SIP ALG passthrough
VPN	2 IPSec tunnels IKE and Manual Key Management AH and ESP Protocol DES, 3DES and AES Encryption SHA-1 and MD5 Authentication Tunnel and Transport Mode Encapsulation IPSec NAT Traversal NETBIOS pass-through for IPSec

### 31.3 Voice Specifications



To take full advantage of the supplementary phone services available through the ZyXEL Device's phone ports, you may need to subscribe to the services from your VoIP service provider.



Not all features are supported by all service providers. Consult your service provider for more information.

**Table 185** Voice Features

Call Fallback	Call fallback allows you to set the ZyXEL Device to automatically use the PSTN/ISDN connection for outgoing calls if the SIP account is not working, or to use the SIP account for outgoing calls if the PSTN/ISDN port is unplugged or not working.
Call Park and Pickup	Call park and pickup lets you put a call on hold (park) and then continue the call (pickup). You can continue the call on the same phone, or another phone connected to the ZyXEL Device. The caller must still pay while the call is parked.  When you park the call, you enter a number of your choice (up to eight digits), which you must enter again when you pick up the call. If you do not enter the correct number, you cannot pickup the call. This means that only someone who knows the number you have chosen can pick up the call.  You can have more than one call on hold at the same time, but you must give each call a different number.
Call Return	With call return, you can place a call to the last number that called you (either answered or missed). The last incoming call can be through either SIP or PSTN.

**Table 185** Voice Features

Country Code	Phone standards and settings differ from one country to another, so the settings on your ZyXEL Device must be configured to match those of the country you are in. The country code feature allows you to do this by selecting the country from a list rather than changing each setting manually. Configure the country code feature when you move the ZyXEL Device from one country to another.
Distinctive Ringing	With the distinctive ring feature, you can assign different ringing tones to different incoming calls, based either on the number that calls you or from where the call originates (SIP, PSTN or internal). Use this feature to let you know where a call comes from before you answer it.
Do not Disturb (DnD)	This feature allows you to set your phone not to ring when someone calls you. You can set each phone independently using its keypad, or configure global settings for all phones using the command line interpreter.
Hot Line	You can set the ZyXEL Device to automatically dial a specified number immediately whenever you lift a phone off the hook. Use the Web Configurator to set the specified number. Use the command line interpreter to have the ZyXEL Device wait a specified length of time before dialing the number.
Music on hold	This feature allows you to put a call on hold and have the other person hear a piece of audio (music, speech, etc.) you previously recorded.
Phone config	The phone config table allows you to customize the phone keypad combinations you use to access certain features on the ZyXEL Device, such as call waiting, call return, call forward, etc. The phone config table is configurable in command interpreter mode.
Internal call	When you have phones attached to both of the ZyXEL Device's phone ports, you can dial "####" to call all the phones connecting to the ZyXEL Device's phone ports. You can also assign each phone connected to the ZyXEL Device an extension number and place a internal call to a specific phone.
HTTP Pincode	When new firmware is available for your ZyXEL Device, you hear a recorded message when you pick up the phone. Enter *99# in your phone's keypad to have the ZyXEL Device upgrade the firmware, or enter #99# to not upgrade. If your service provider gave you different numbers to use, enter them instead. If you enter the code to not upgrade, you can make a call as normal. You will hear the recording again each time you pick up the phone, until you upgrade.
Call waiting	This feature allows you to hear an alert when you are already using the phone and another person calls you. You can then either reject the new incoming call, put your current call on hold and receive the new incoming call, or end the current call and receive the new incoming call.
Call forwarding	With this feature, you can set the ZyXEL Device to forward calls to a specified number, either unconditionally (always), when your number is busy, or when you do not answer. You can also forward incoming calls from one specified number to another.
Caller ID	The ZyXEL Device supports caller ID, which allows you to see the originating number of an incoming call (on a phone with a suitable display).
Trunking	Trunking connects an IP network (like the Internet) with the regular telephone network (PSTN). The main advantage of trunking is that you can call your ZyXEL Device on the PSTN network, and then use it to make a VoIP phonecall. For example, if you have a ZyXEL Device at your office you can call into it from your cellphone and use it to make a long-distance or international VoIP call at a reduced cost.
REN	A Ringer Equivalence Number (REN) is used to determine the number of devices (like telephones or fax machines) that may be connected to the telephone line. Your device has a REN of three, so it can support three devices per telephone port.
Dynamic Jitter Buffer	The built-in adaptive buffer helps to smooth out the variations in delay (jitter) for voice traffic. This helps ensure good voice quality for your conversations.

**Table 185** Voice Features

Multiple SIP Accounts	You can simultaneously use multiple voice (SIP) accounts and assign them to one or both telephone ports.
Multiple Voice Channels	Your device can simultaneously handle multiple voice channels (telephone calls). Additionally you can answer an incoming phone call on a VoIP account, even while someone else is using the account for a phone call.
Voice Activity Detection/Silence Suppression	Voice Activity Detection (VAD) reduces the bandwidth that a call uses by not transmitting when you are not speaking.
Comfort Noise Generation	Your device generates background noise to fill moments of silence when the other device in a call stops transmitting because the other party is not speaking (as total silence could easily be mistaken for a lost connection).
Echo Cancellation	Your device supports G.168, an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
QoS (Quality of Service)	Quality of Service (QoS) mechanisms help to provide better service on a per-flow basis. Your device supports Type of Service (ToS) tagging and Differentiated Services (DiffServ) tagging. This allows the device to tag voice frames so they can be prioritized over the network.
MSNs	You can use MSNs (Multiple Subscriber Numbers) to identify individual ISDN phone connected to the ZyXEL Device for internal calls. Configure MSNs in the ZyXEL Device allow analog phones to use MSN features in ISDN calls.
SIP ALG	Your device is a SIP Application Layer Gateway (ALG). It allows VoIP calls to pass through NAT for devices behind it (such as a SIP-based VoIP software application on a computer).
Other Voice Features	SIP version 2 (Session Initiating Protocol RFC 3261) SDP (Session Description Protocol RFC 2327) RTP (RFC 1889) RTCP (RFC 1890) Voice codecs (coder/decoders) G.711, G.726, G.729 Fax and data modem discrimination DTMF Detection and Generation DTMF: In-band and Out-band traffic (RFC 2833),(PCM), (SIP INFO) Point-to-point call establishment between two IADs Quick dialing through predefined phone book, which maps the phone dialing number and destination URL. Flexible Dial Plan (RFC3525 section 7.1.14)

### 31.4 Wireless Features (Wireless Devices Only)

**Table 186** Wireless Features

IEEE 802.11g+ Wireless LAN	Your device supports IEEE 802.11g+ to allow any ZyXEL WLAN devices that also support IEEE 802.1g+ to associate with the ZyXEL Device at higher transmission speeds than with standard IEEE 802.11g.
External Antenna	The ZyXEL Device is equipped with an attached antenna to provide a clear radio signal between the wireless stations and the access points.
Wireless LAN MAC Address Filtering	Your device can check the MAC addresses of wireless stations against a list of allowed or denied MAC addresses.

**Table 186** Wireless Features

Association List	This feature allows you to know which wireless stations are currently associated with the ZyXEL Device. You can block the individual wireless station in the association list screen from accessing the ZyXEL Device.
WEP Encryption	WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network to help keep network communications private.
Wi-Fi Protected Access	Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security standard. Key differences between WPA and WEP are user authentication and improved data encryption.
WPA2	WPA 2 is a wireless security standard that defines stronger encryption, authentication and key management than WPA.
WDS	Use the WDS (Wireless Distribution System) to secure the link between the ZyXEL Device and other APs on your network. At the time of writing, the ZyXEL Device only supports WDS links with other ZyXEL Devices.
WMM QoS	WMM (Wi-Fi MultiMedia) QoS (Quality of Service) allows you to prioritize wireless traffic according to the delivery requirements of individual services.
Other Wireless Features	IEEE 802.11g Compliance Frequency Range: 2.4 GHz ISM Band Advanced Orthogonal Frequency Division Multiplexing (OFDM) Data Rates: 54Mbps, 11Mbps, 5.5Mbps, 2Mbps, and 1 Mbps Auto Fallback Turn on-off WLAN by reset button (press 1s on reset button to turn on or turn off the WLAN; 5s for OTIST; 10s to reset back to factory default) WPA2 WMM IEEE 802.11i IEEE 802.11e Wired Equivalent Privacy (WEP) Data Encryption 64/128/256 bit. WLAN bridge to LAN Up to 32 MAC Address filters IEEE 802.1x Store up to 32 built-in user profiles using EAP-MD5 (Local User Database) External RADIUS server using EAP-MD5, TLS, TTLS OTIST (ZyXEL's One-Touch Intelligent Security Technology)

### 31.4.1 IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b radio card can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

**Table 187** IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)

**Table 187 IEEE 802.11g**

DATA RATE (MBPS)	MODULATION
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)



Your device may be prone to RF (Radio Frequency) interference from other 2.4 GHz devices such as microwave ovens, wireless phones, Bluetooth enabled devices, and other wireless LANs.

## 31.5 Power Adaptor Specifications

**Table 188 P-2602HWL Series Power Adaptor Specifications**

North American PLUG standards	OEM (Original Equipment Manufacturer)	LEI (LEADER ELECTRONICS INC.)
AC Power Adapter Model	ADS18B-W 180100	MU18-2180100-A1
Input Power	AC 100~240Volts/50/60Hz/0.5A	AC 100~240Volts/50/60Hz/0.6A
Output Power	DC 18Volts/1A	DC 18Volts/1A
Power Consumption	12 Watt max	12 Watt max
Safety Standards	UL,CUL(UL 60950-1)	UL,CUL(UL 60950-1)
EUROPEAN PLUG STANDARDS		
AC Power Adapter Model	ADS18B-B 180100	MU18-2180100-C5
Input Power	AC 100~240Volts/50/60Hz/0.5A	AC 100~240Volts/50/60Hz/0.6A
Output Power	DC 18Volts/1A	DC 18Volts/1A
Power Consumption	12 Watt max	12 Watt max
Safety Standards	TUV, CE(EN 60950 -1 )	TUV, CE(EN 60950-1)
UNITED KINGDOM PLUG STANDARDS		
AC Power Adapter Model	ADS18B-D 180100	MU18-2180100-B2
Input Power	AC 100~240Volts/50/60Hz/0.5A	AC 100~240Volts/50/60Hz/0.6A
Output Power	DC 18Volts/1A	DC 18Volts/1A
Power Consumption	12 Watt max	12 Watt max
Safety Standards	TUV, CE(EN 60950 -1 )	TUV, CE(EN 60950-1)



---

# PART VIII

# Appendices and

# Index

---

- Setting up Your Computer's IP Address (435)
- Pop-up Windows, JavaScripts and Java Permissions (447)
- IP Addresses and Subnetting (453)
- Wireless LANs (461)
- Services (475)
- Legal Information (479)
- Customer Support (483)
- Index (489)



# Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

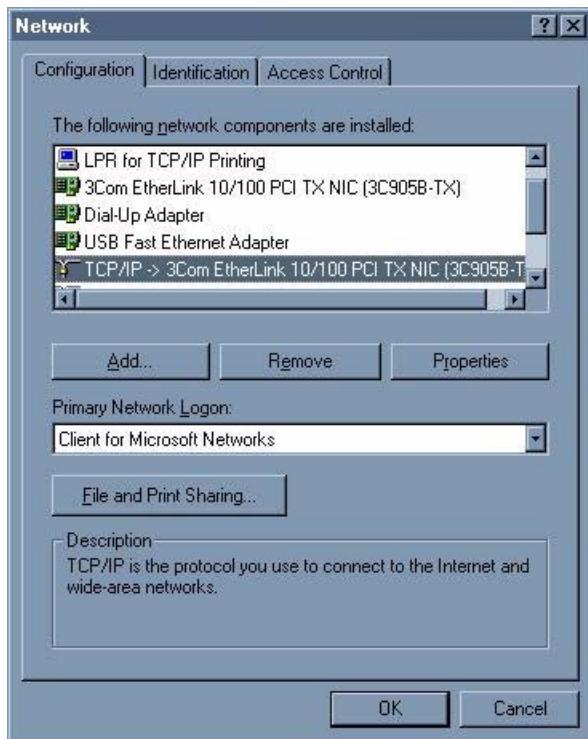
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the ZyXEL Device's LAN port.

## Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window

**Figure 249** Windows 95/98/Me: Network: Configuration



## Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

- 1 In the **Network** window, click **Add**.
- 2 Select **Adapter** and then click **Add**.
- 3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

- 1 In the **Network** window, click **Add**.
- 2 Select **Protocol** and then click **Add**.
- 3 Select **Microsoft** from the list of **manufacturers**.
- 4 Select **TCP/IP** from the list of network protocols and then click **OK**.

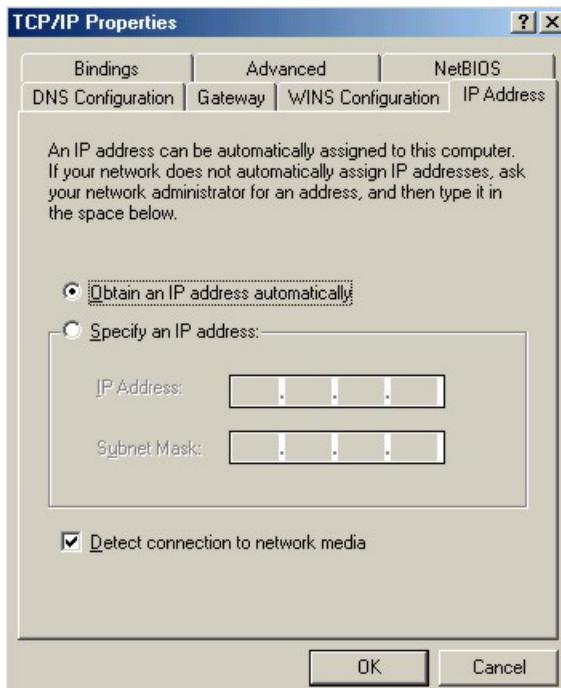
If you need Client for Microsoft Networks:

- 1 Click **Add**.
- 2 Select **Client** and then click **Add**.
- 3 Select **Microsoft** from the list of manufacturers.
- 4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- 5 Restart your computer so the changes you made take effect.

## Configuring

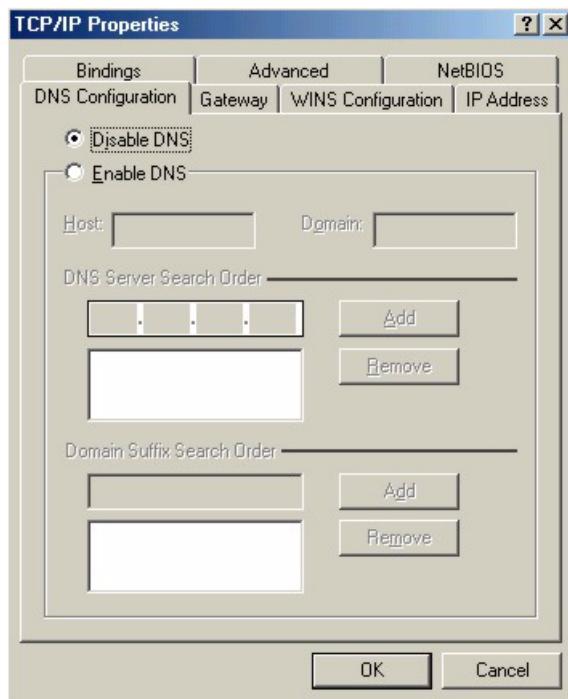
- 1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
- 2 Click the **IP Address** tab.
  - If your IP address is dynamic, select **Obtain an IP address automatically**.
  - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

**Figure 250** Windows 95/98/Me: TCP/IP Properties: IP Address



- 3 Click the **DNS Configuration** tab.
  - If you do not know your DNS information, select **Disable DNS**.
  - If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

**Figure 251** Windows 95/98/Me: TCP/IP Properties: DNS Configuration



- 4 Click the **Gateway** tab.
  - If you do not know your gateway's IP address, remove previously installed gateways.
  - If you have a gateway IP address, type it in the **New gateway** field and click **Add**.
- 5 Click **OK** to save and close the **TCP/IP Properties** window.
- 6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
- 7 Turn on your ZyXEL Device and restart your computer when prompted.

## Verifying Settings

- 1 Click **Start** and then **Run**.
- 2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
- 3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

## Windows 2000/NT/XP

- 1 For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

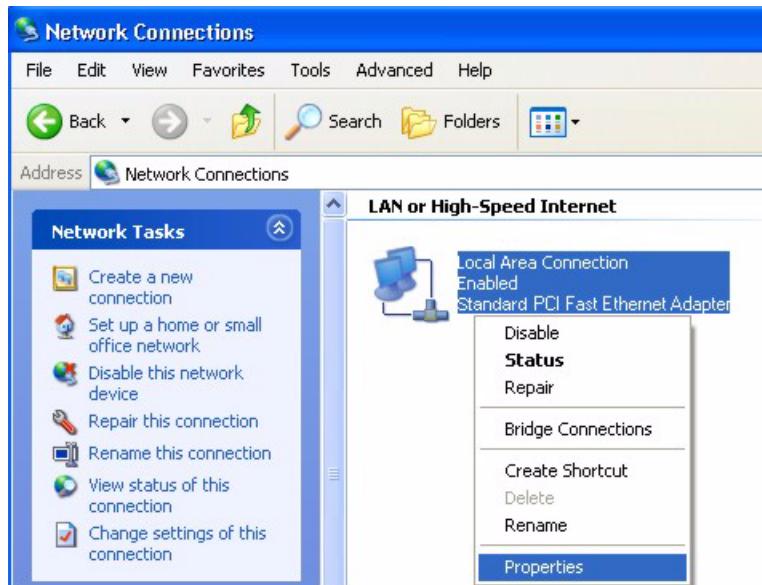
**Figure 252** Windows XP: Start Menu

- 2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

**Figure 253** Windows XP: Control Panel

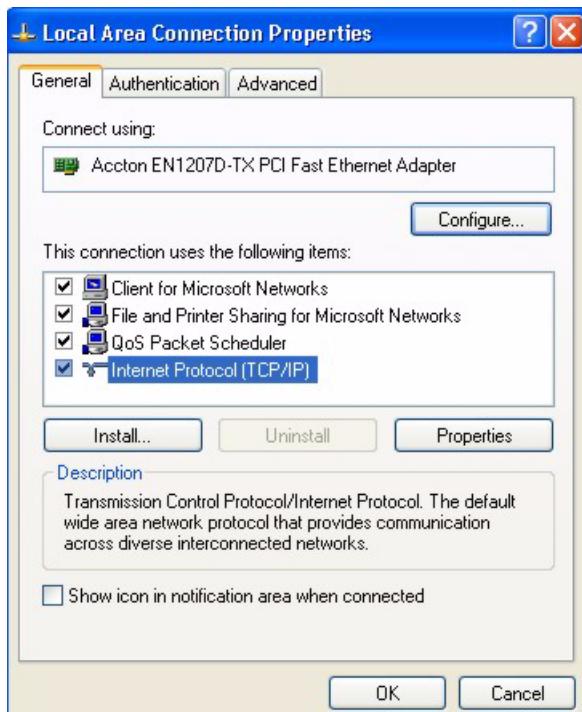
- 3 Right-click **Local Area Connection** and then click **Properties**.

**Figure 254** Windows XP: Control Panel: Network Connections: Properties

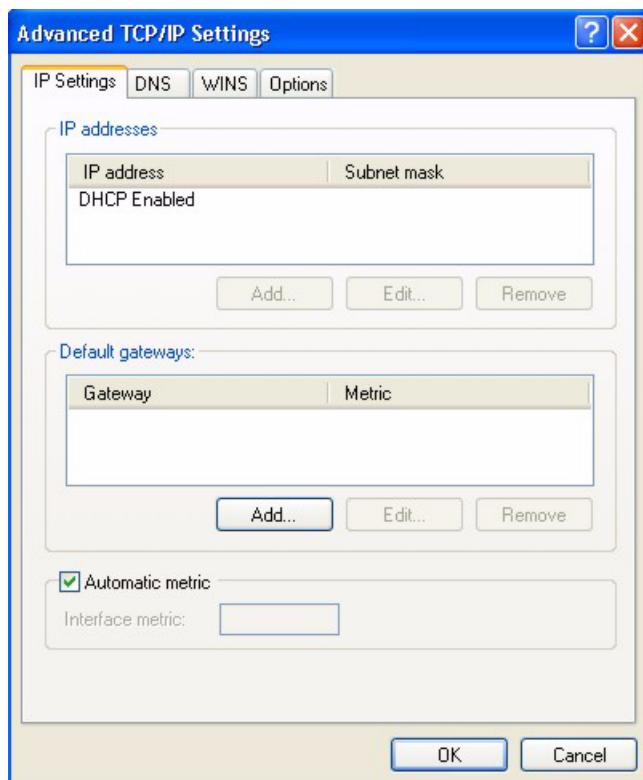


- 4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and click **Properties**.

**Figure 255** Windows XP: Local Area Connection Properties



- 5 The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).
  - If you have a dynamic IP address click **Obtain an IP address automatically**.
  - If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields. Click **Advanced**.

**Figure 256** Windows XP: Advanced TCP/IP Settings

- 6** If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

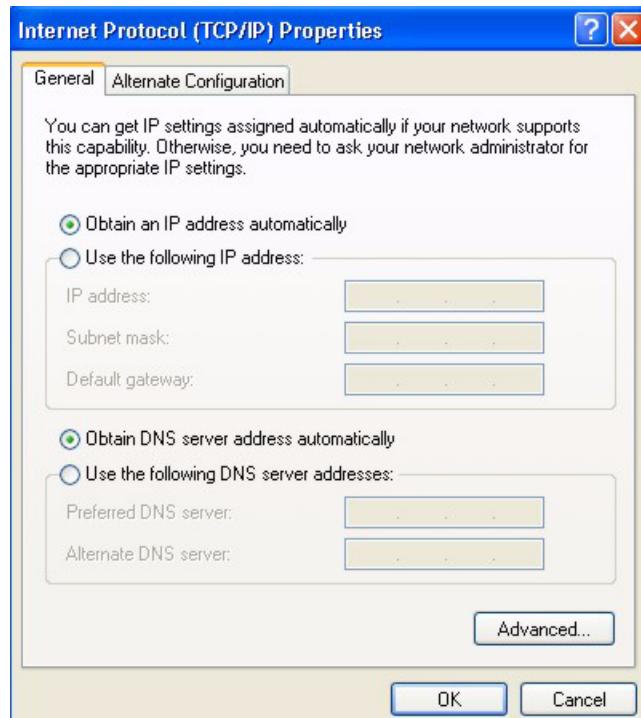
Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

- 7** In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):
- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
  - If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

**Figure 257** Windows XP: Internet Protocol (TCP/IP) Properties



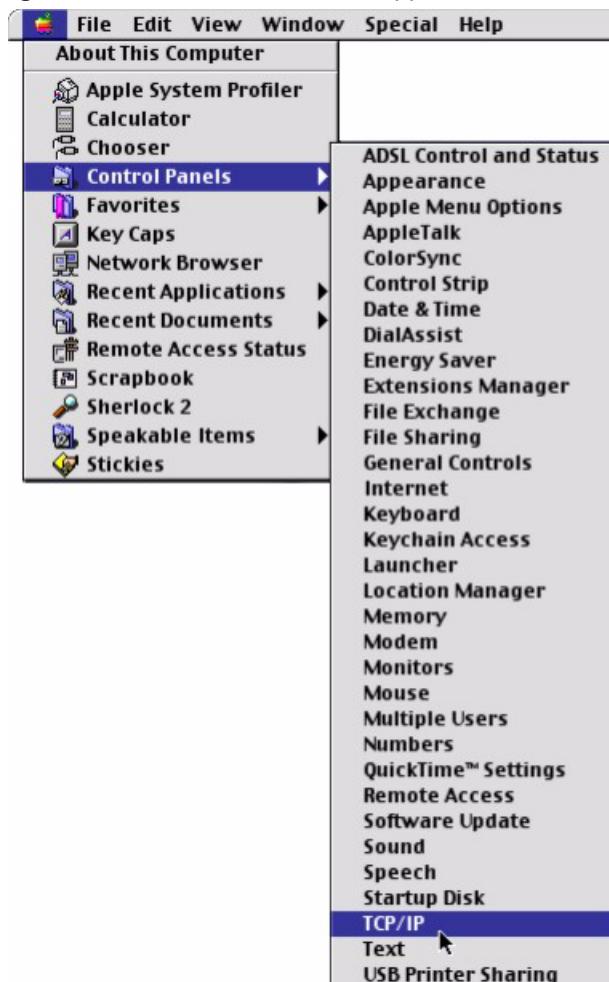
- 8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 9 Click **OK** to close the **Local Area Connection Properties** window.
- 10 Turn on your ZyXEL Device and restart your computer (if prompted).

## Verifying Settings

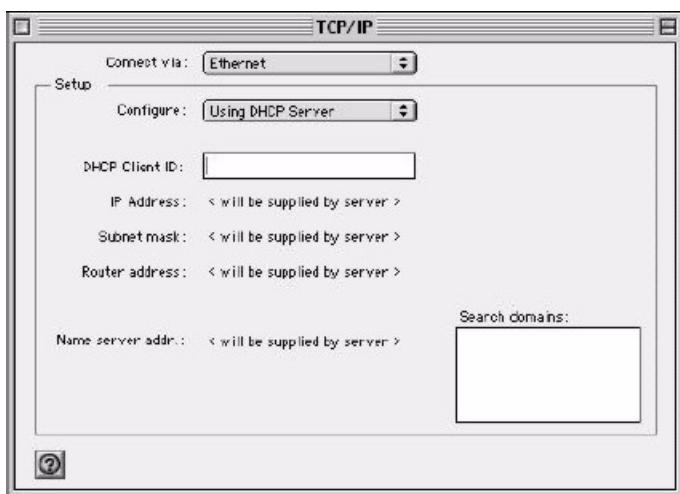
- 1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

## Macintosh OS 8/9

- 1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

**Figure 258** Macintosh OS 8/9: Apple Menu

**2** Select **Ethernet built-in** from the **Connect via** list.

**Figure 259** Macintosh OS 8/9: TCP/IP

**3** For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

- 4** For statically assigned settings, do the following:
  - From the **Configure** box, select **Manually**.
  - Type your IP address in the **IP Address** box.
  - Type your subnet mask in the **Subnet mask** box.
  - Type the IP address of your ZyXEL Device in the **Router address** box.
- 5** Close the **TCP/IP Control Panel**.
- 6** Click **Save** if prompted, to save changes to your configuration.
- 7** Turn on your ZyXEL Device and restart your computer (if prompted).

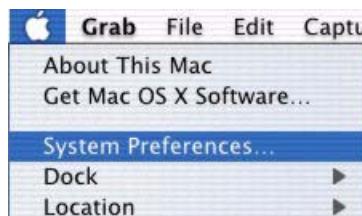
## Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

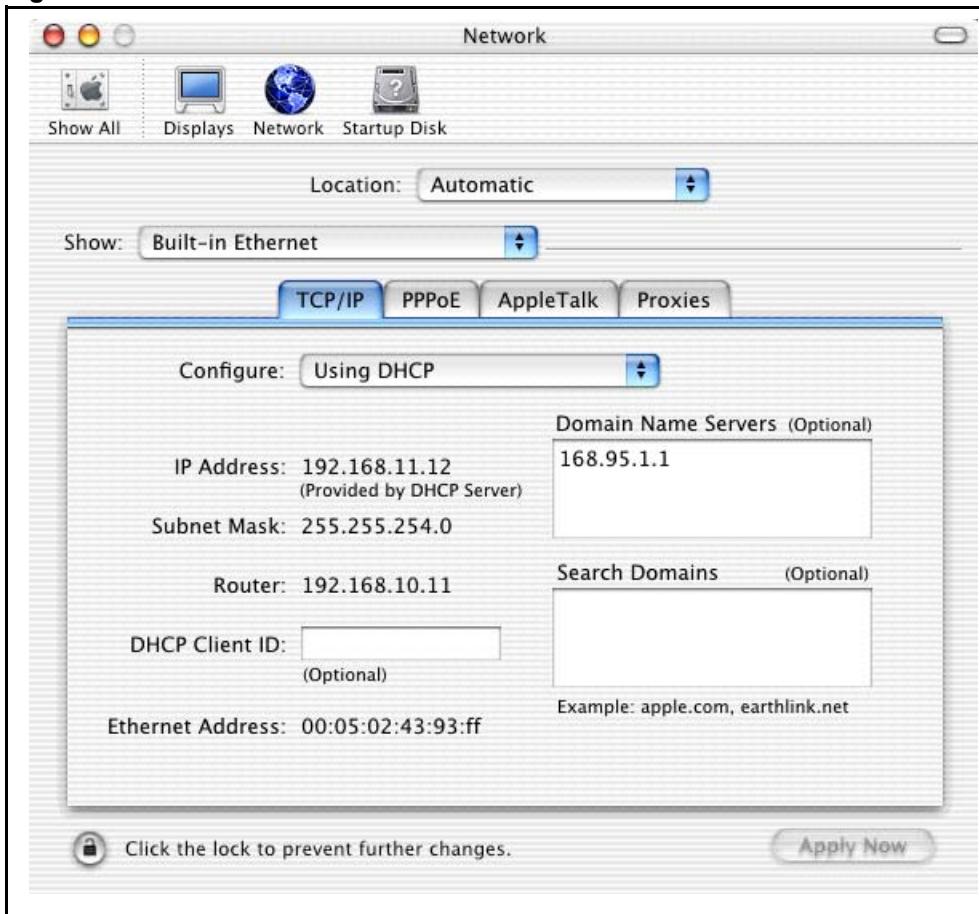
## Macintosh OS X

- 1** Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

**Figure 260** Macintosh OS X: Apple Menu



- 2** Click **Network** in the icon bar.
  - Select **Automatic** from the **Location** list.
  - Select **Built-in Ethernet** from the **Show** list.
  - Click the **TCP/IP** tab.
- 3** For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

**Figure 261** Macintosh OS X: Network

- 4 For statically assigned settings, do the following:
  - From the **Configure** box, select **Manually**.
  - Type your IP address in the **IP Address** box.
  - Type your subnet mask in the **Subnet mask** box.
  - Type the IP address of your ZyXEL Device in the **Router address** box.
- 5 Click **Apply Now** and close the window.
- 6 Turn on your ZyXEL Device and restart your computer (if prompted).

## Verifying Settings

Check your TCP/IP properties in the **Network** window.



# Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).




---

**Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.**

---

## Internet Explorer Pop-up Blockers

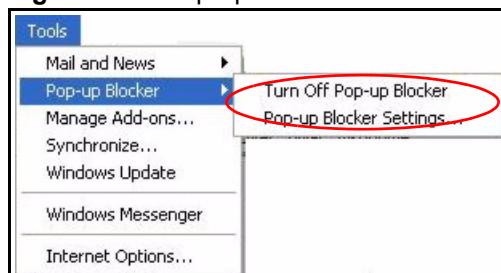
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

### Disable pop-up Blockers

- 1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

**Figure 262** Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

- 1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

- 2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

**Figure 263** Internet Options: Privacy

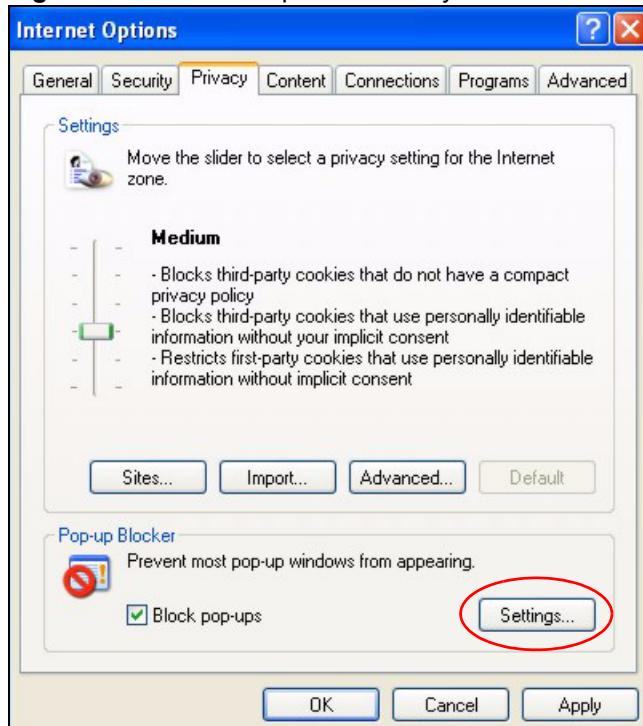


- 3 Click **Apply** to save this setting.

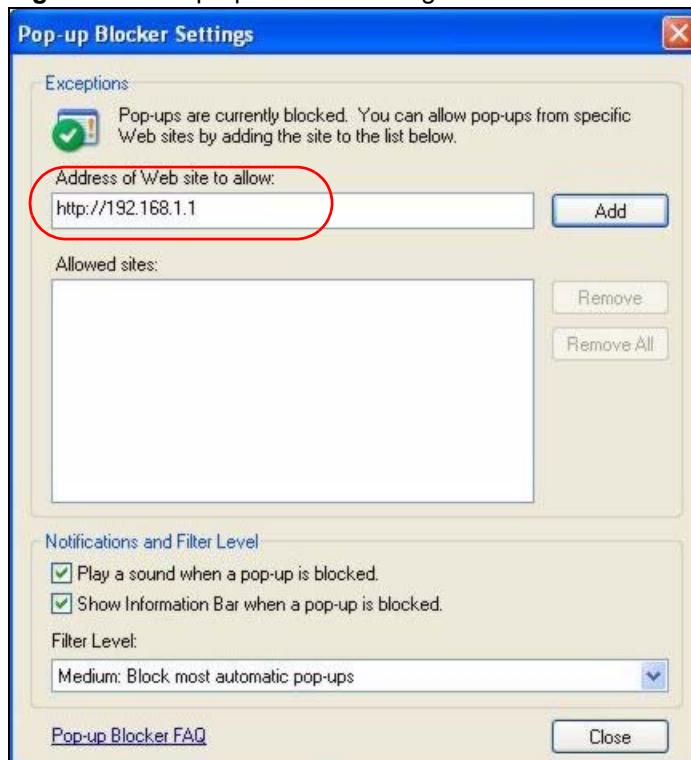
### Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

- 1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.
- 2 Select **Settings...** to open the **Pop-up Blocker Settings** screen.

**Figure 264** Internet Options: Privacy

- 3** Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.167.1.
- 4** Click **Add** to move the IP address to the list of **Allowed sites**.

**Figure 265** Pop-up Blocker Settings

**5** Click **Close** to return to the **Privacy** screen.

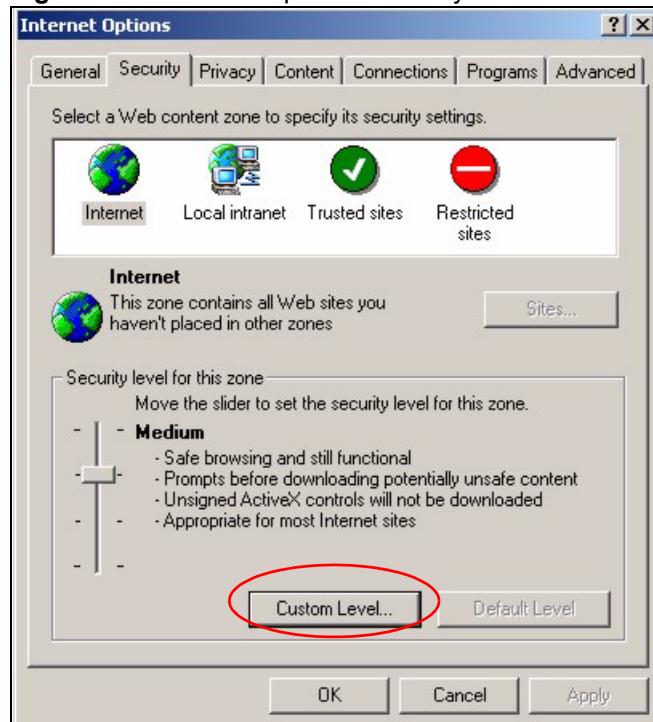
**6** Click **Apply** to save this setting.

## JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

**1** In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

**Figure 266** Internet Options: Security



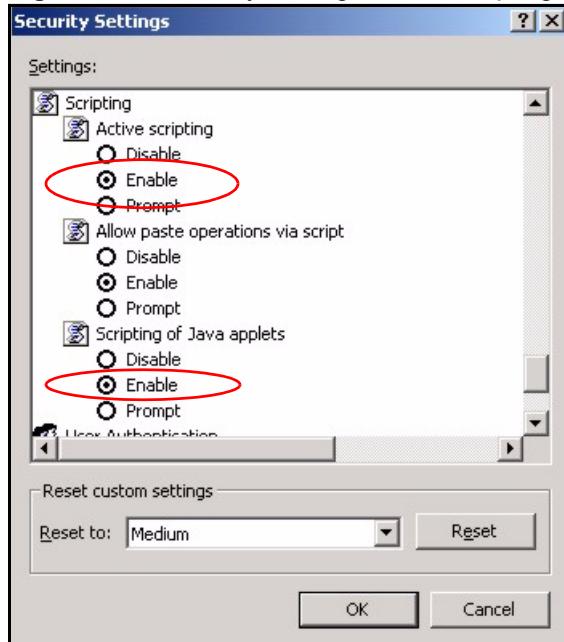
**2** Click the **Custom Level...** button.

**3** Scroll down to **Scripting**.

**4** Under **Active scripting** make sure that **Enable** is selected (the default).

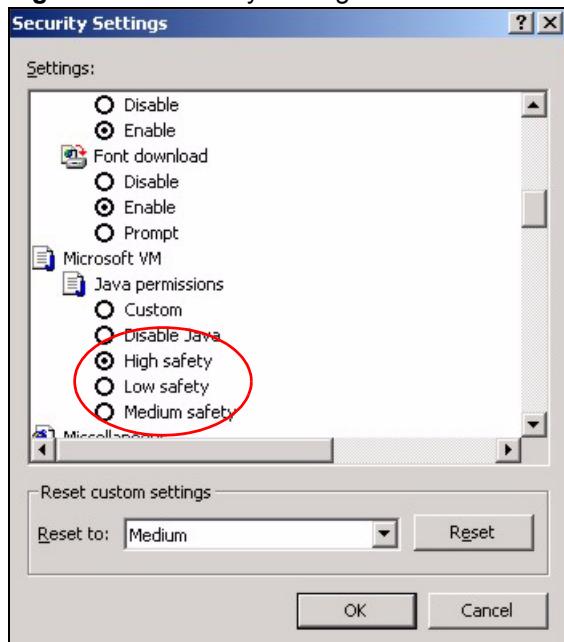
**5** Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

**6** Click **OK** to close the window.

**Figure 267** Security Settings - Java Scripting

## Java Permissions

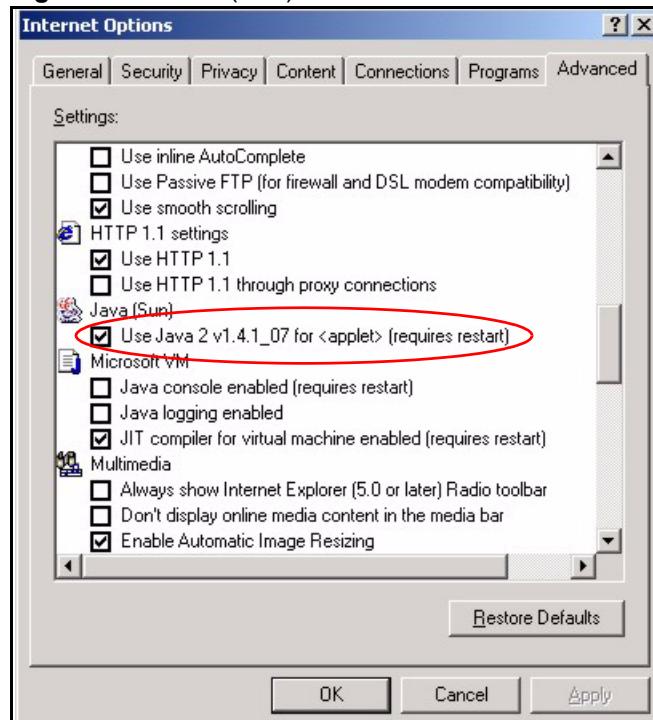
- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.
- 5 Click **OK** to close the window.

**Figure 268** Security Settings - Java

## JAVA (Sun)

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Advanced** tab.
- 2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
- 3 Click **OK** to close the window.

**Figure 269 Java (Sun)**



# IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

## Introduction to IP Addresses

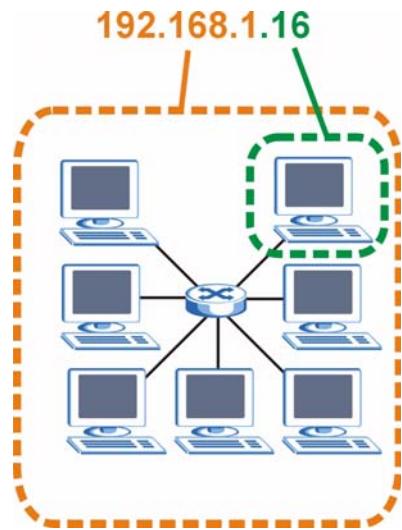
One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

## Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

**Figure 270** Network Number and Host ID

How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

## Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

**Table 189** Subnet Masks

	<b>1ST OCTET: (192)</b>	<b>2ND OCTET: (168)</b>	<b>3RD OCTET: (1)</b>	<b>4TH OCTET (2)</b>
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	<b>11111111</b>	<b>11111111</b>	<b>11111111</b>	00000000
Network Number	<b>11000000</b>	<b>10101000</b>	<b>00000001</b>	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

**Table 190** Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11110000	255.255.255.248

## Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

**Table 191** Maximum Host Numbers

SUBNET MASK	HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$
16 bits	255.255.0.0	16 bits	$2^{16} - 2$
24 bits	255.255.255.0	8 bits	$2^8 - 2$
29 bits	255.255.255.248	3 bits	$2^3 - 2$

## Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

**Table 192** Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128

**Table 192** Alternative Subnet Mask Notation (continued)

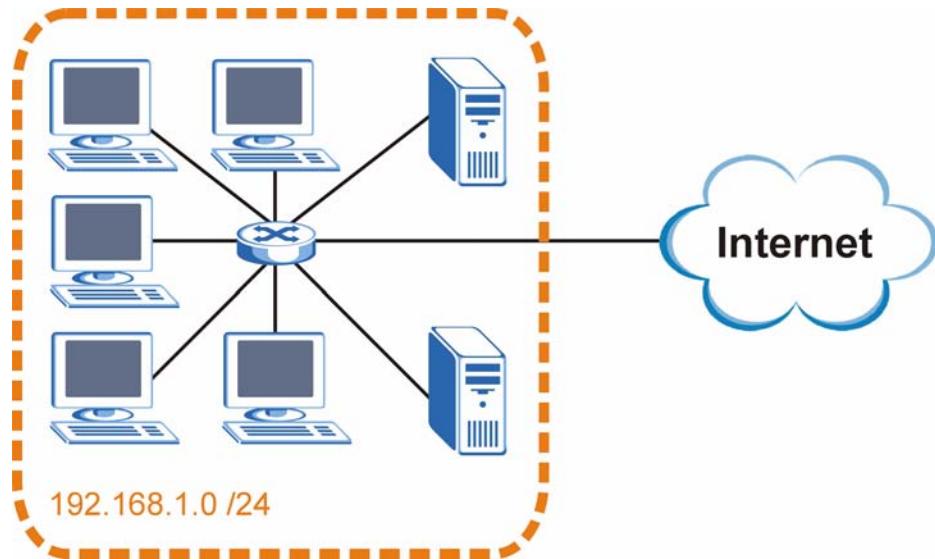
SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

## Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of  $2^8 - 2$  or 254 possible hosts.

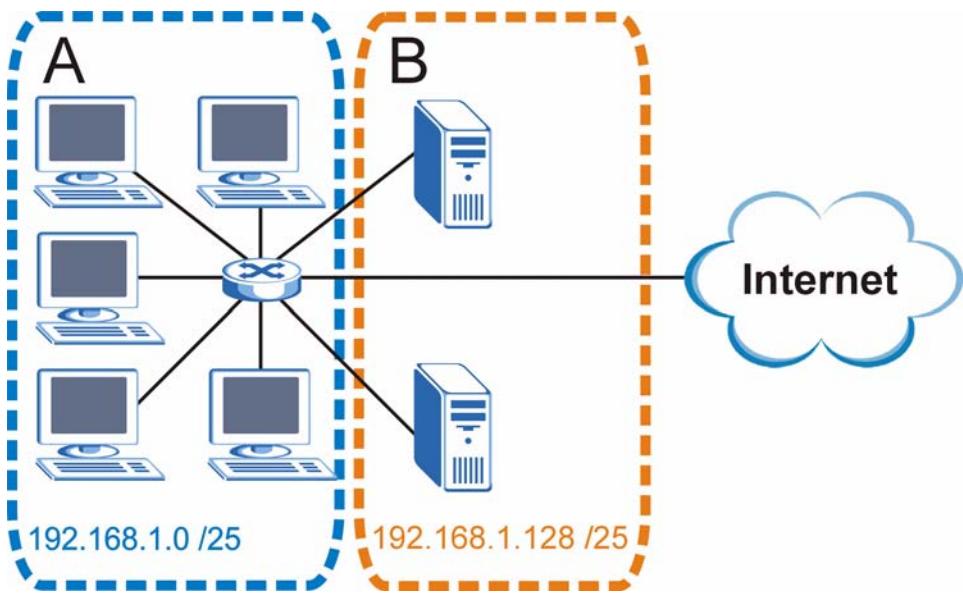
The following figure shows the company network before subnetting.

**Figure 271** Subnetting Example: Before Subnetting

You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

**Figure 272** Subnetting Example: After Subnetting

In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of  $2^7 - 2$  or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

## Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to “borrow” two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11000000**) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving  $2^6 - 2$  or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

**Table 193** Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	<b>00000000</b>
Subnet Mask (Binary)	11111111.11111111.11111111.	<b>11000000</b>
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

**Table 194** Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	01000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

**Table 195** Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

**Table 196** Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	11000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

## Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

**Table 197** Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127

**Table 197** Eight Subnets (continued)

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

## Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

**Table 198** 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

**Table 199** 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6

**Table 199** 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

## Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the ZyXEL Device.

Once you have decided on the network number, pick an IP address for your ZyXEL Device that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

### Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space*.

# Wireless LANs

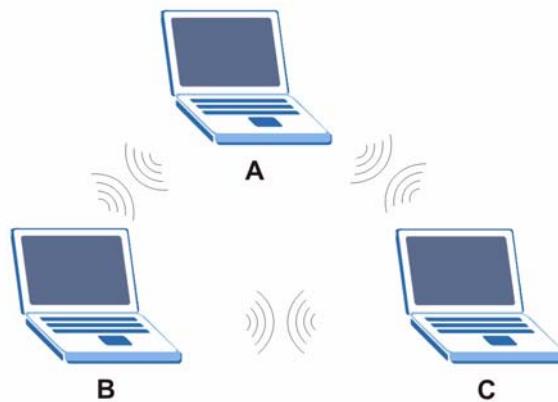
## Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

### Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

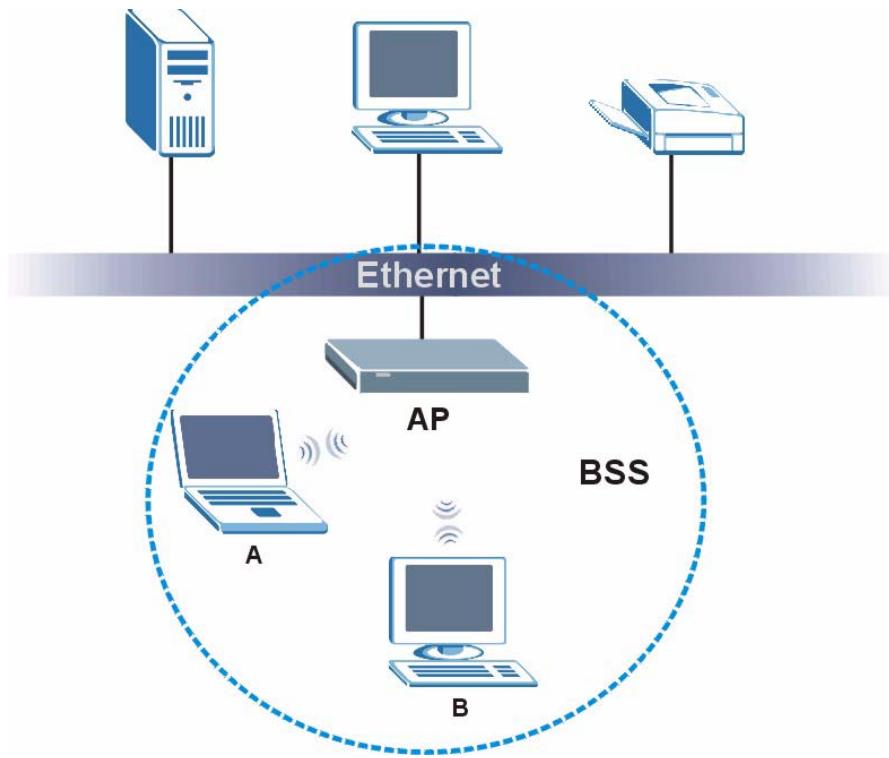
**Figure 273** Peer-to-Peer Communication in an Ad-hoc Network



### BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

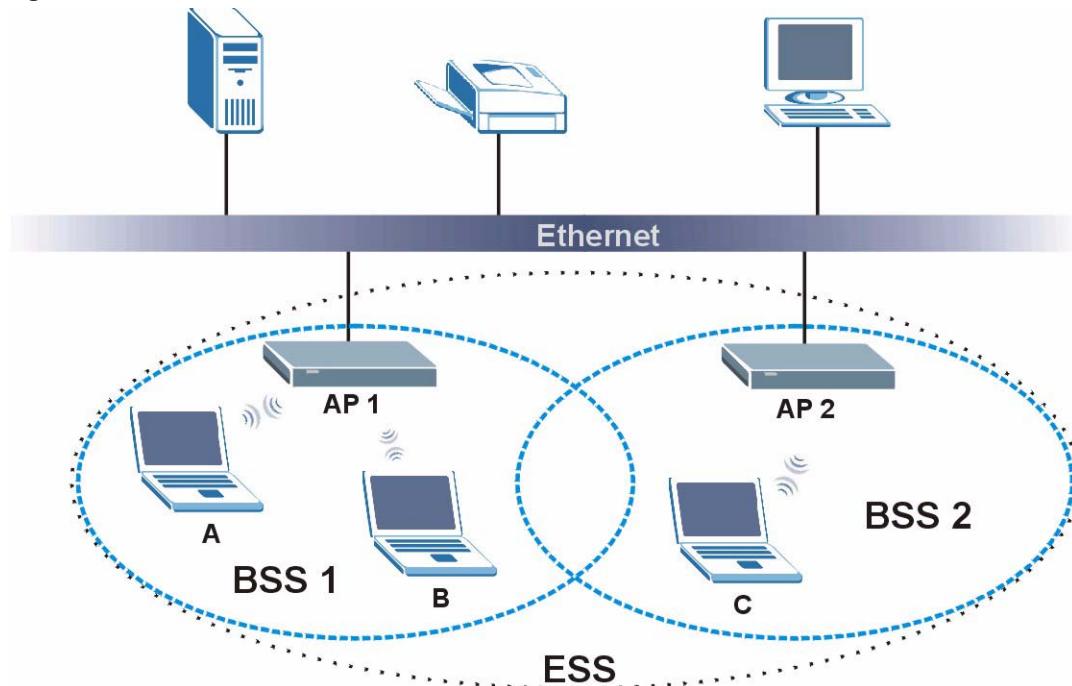
**Figure 274** Basic Service Set

## ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

**Figure 275** Infrastructure WLAN

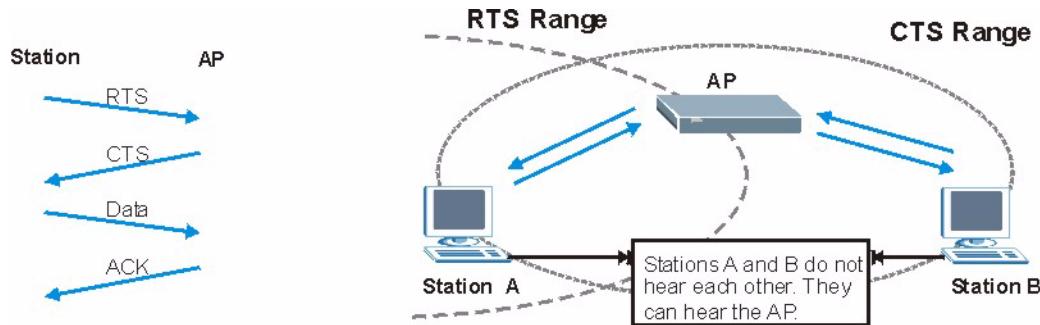
## Channel

A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

## RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

**Figure 276** RTS/CTS

When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

**RTS/CTS** is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.



Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

## Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

## Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks.

Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the Product Name [short] uses long preamble.




---

The wireless devices **MUST** use the same preamble mode in order to communicate.

---

## IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

**Table 200** IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

## Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the Product Name [short] are data encryption, wireless client authentication, restricting access by device MAC address and hiding the Product Name [short] identity.

The following figure shows the relative effectiveness of these wireless security methods available on your Product Name [short].

**Table 201** Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
	WPA2



You must enable the same wireless security settings on the Product Name [short] and on all wireless clients that you want to associate with it.

## IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

## RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication  
Determines the identity of the users.
- Authorization

Determines the network services available to authenticated users once they are connected to the network.

- Accounting  
Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

## Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request  
Sent by an access point requesting authentication.
- Access-Reject  
Sent by a RADIUS server rejecting access.
- Access-Accept  
Sent by a RADIUS server allowing access.
- Access-Challenge  
Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request  
Sent by the access point requesting accounting.
- Accounting-Response  
Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

## Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x..

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

### **EAP-MD5 (Message-Digest Algorithm 5)**

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client ‘proves’ that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

### **EAP-TLS (Transport Layer Security)**

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender’s identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

### **EAP-TTLS (Tunneled Transport Layer Service)**

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

### **PEAP (Protected EAP)**

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

### **LEAP**

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

## Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.




---

### EAP-MD5 cannot be used with Dynamic WEP Key Exchange

---

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

**Table 202** Comparison of EAP Authentication Types

	<b>EAP-MD5</b>	<b>EAP-TLS</b>	<b>EAP-TTLS</b>	<b>PEAP</b>	<b>LEAP</b>
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

## WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

## Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

## User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

## Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

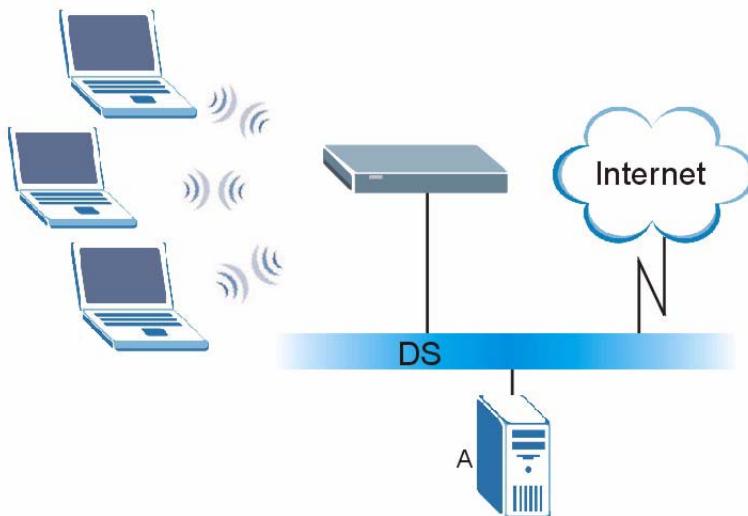
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

## WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

- 1 The AP passes the wireless client's authentication request to the RADIUS server.
- 2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
- 3 A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.
- 4 The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

**Figure 277** WPA(2) with RADIUS Application Example

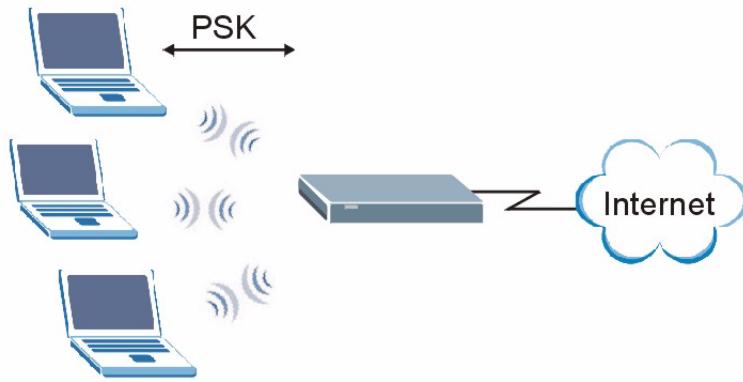


## WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

- 1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
- 2 The AP checks each wireless client's password and allows it to join the network only if the password matches.

- 3 The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.
- 4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

**Figure 278** WPA(2)-PSK Authentication

## Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

**Table 203** Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

## Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

## Antenna Characteristics

### Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

### Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

### Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

## Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

## Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to-point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

# Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name:** This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol:** This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s):** This value depends on the **Protocol**.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description:** This is a brief explanation of the applications that use this service or the situations in which this service is used.

**Table 204** Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL's Internet Messenger service.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP/UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for instance <a href="http://www.zyxel.com">www.zyxel.com</a> ) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Protocol, a program to enable fast transfer of files, including large files that may not be possible by e-mail.

**Table 204** Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IMAP4	TCP	143	The Internet Message Access Protocol is used for e-mail.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	The Network Basic Input/Output System is used for communication between computers in a LAN.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.

**Table 204** Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
RExec	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	The Simple File Transfer Protocol is an old way of transferring files between computers.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.

**Table 204** Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP UDP	7000 user-defined	A videoconferencing solution. The UDP port number is specified in the application.

# Legal Information

## Copyright

Copyright © 2006 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

## Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

## Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

## Certifications

### Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- 1 Reorient or relocate the receiving antenna.
- 2 Increase the separation between the equipment and the receiver.
- 3 Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- 4 Consult the dealer or an experienced radio/TV technician for help.



### FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

## 注意！

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。  
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。  
減少電磁波影響，請妥適使用。

### Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

### Viewing Certifications

- 1 Go to <http://www.zyxel.com>.

- 2** Select your product on the ZyXEL home page to go to that product's page.
- 3** Select the certification you wish to view from this page.

## ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

### Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

### Registration

Register your product online to receive e-mail notices of firmware upgrades and information at [www.zyxel.com](http://www.zyxel.com) for global products, or at [www.us.zyxel.com](http://www.us.zyxel.com) for North American products.



# Customer Support

Please have the following information ready when you contact customer support.

## Required Information

- Product model and serial number.
  - Warranty Information.
  - Date that you received your device.
  - Brief description of the problem and the steps you took to solve it.
- “+” is the (prefix) number you dial to make an international telephone call.

## Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: www.zyxel.com, www.europe.zyxel.com
- FTP: ftp.zyxel.com, ftp.europe.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

## Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web: www.zyxel.co.cr
- FTP: ftp.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

## Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: www.zyxel.cz

- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Česká Republika

### **Denmark**

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

### **Finland**

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780-8448
- Web: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

### **France**

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

### **Germany**

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

### **Hungary**

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

**India**

- Support E-mail: support@zyxel.in
- Sales E-mail: sales@zyxel.in
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: <http://www.zyxel.in>
- Regular Mail: India - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

**Japan**

- Support E-mail: support@zyxel.co.jp
- Sales E-mail: zyp@zyxel.co.jp
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: [www.zyxel.co.jp](http://www.zyxel.co.jp)
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

**Kazakhstan**

- Support: <http://zyxel.kz/support>
- Sales E-mail: sales@zyxel.kz
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: [www.zyxel.kz](http://www.zyxel.kz)
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

**Malaysia**

- Support E-mail: support@zyxel.com.my
- Sales E-mail: sales@zyxel.com.my
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: <http://www.zyxel.com.my>
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

**North America**

- Support E-mail: support@zyxel.com
- Support Telephone: +1-800-978-7222
- Sales E-mail: sales@zyxel.com
- Sales Telephone: +1-714-632-0882
- Fax: +1-714-632-0858
- Web: [www.zyxel.com](http://www.zyxel.com)

- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

### **Norway**

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

### **Poland**

- E-mail: info@pl.zyxel.com
- Telephone: +48-22-333 8250
- Fax: +48-22-333 8251
- Web: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzesi 1A, 03-715 Warszawa, Poland

### **Russia**

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow 117279, Russia

### **Singapore**

- Support E-mail: support@zyxel.com.sg
- Sales E-mail: sales@zyxel.com.sg
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: http://www.zyxel.com.sg
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

### **Spain**

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5<sup>a</sup> planta, 28033 Madrid, Spain

**Sweden**

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

**Thailand**

- Support E-mail: support@zyxel.co.th
- Sales E-mail: sales@zyxel.co.th
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: http://www.zyxel.co.th
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

**Ukraine**

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

**United Kingdom**

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344-303044, 08707-555779 (UK only)
- Fax: +44-1344-303034
- Web: www.zyxel.co.uk
- FTP: ftp.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)



# Index

## A

AAL5 **426**  
 ACK message **173**  
 Address Resolution Protocol (ARP) **121**  
 ADSL2 **426**  
 Advanced Encryption Standard  
     See AES.  
 AES **470**  
 AH **271**  
 AH protocol **275**  
 ALG **429**  
 alternative subnet mask notation **455**  
 antenna **423**  
     directional **473**  
     gain **473**  
     omni-directional **473**  
 any IP **121, 425**  
     how it works **121**  
     note **121**  
 any IP setup **123**  
 AP (access point) **463**  
 Application Layer Gateway **429**  
 application-level firewalls **234**  
 applications  
     Internet access **43**  
 Asynchronous Transfer Mode **420**  
 ATC **331**  
 ATM AAL5 **426**  
 ATM Adaptation Layer 5 (AAL5) **102, 426**  
 attack alert **261**  
 attack types **238**  
 authentication header **275**  
 auto attendant, and VoIP trunking **215**  
 auto firmware upgrade **229**  
 Automatic Traffic Classifier  
     see ATC  
 auto-negotiating rate adaptation **426**  
 auto-provisioning **229, 425**

## B

backup **411**

backup type **115**  
 bandwidth management **331**  
 bandwidth manager class configuration **334**  
 bandwidth manager monitor **337**  
 bandwidth manager summary **333**  
 Basic Service Set, See BSS **461**  
 basic wireless security **74**  
 blocking time **260**  
 brute-force attack, **237**  
 BSS **461**  
 BW budget **335**  
 BYE request **173**

## C

CA **468**  
 CA (Certification Authority) **301**  
 call fallback **427**  
 call forwarding **428**  
 call hold **195, 197**  
 call park and pickup **427**  
 call return **427**  
 call rules, and VoIP trunking **213**  
 call service mode **195, 196**  
 call transfer **196, 197**  
 call waiting **196, 197, 428**  
 caller ID **428**  
 CBR (Continuous Bit Rate) **109, 113**  
 CCK **431**  
 certificate  
     details **308**  
 Certificate Authority  
     See CA.  
 certificates **301**  
     advantages **302**  
     and cryptology **301**  
     and directory servers **302, 322**  
     and public-key cryptology **301**  
     and public-private keys **301**  
     and remote hosts **316**  
     and remote management **345**  
     creating **306**  
     file formats **305**  
     generating requests **301**

importing 304  
remote hosts 319  
revoked 302  
trusted CAs 311, 313  
verifying 318  
Certification Authority (CA) 301  
certifications 479  
notices 480  
viewing 480  
change password at login 50  
channel 463  
interference 463  
channel ID 134  
checking the device's IP address 229  
Class of Service 177  
client-server protocol 170  
codecs 429  
comfort noise generation 184, 429  
Complementary Code Keying Modulation 431  
configuration 118  
configuration file 407  
contact information 483  
content filtering 265  
categories 265  
schedule 266  
trusted computers 267  
URL keyword blocking 265  
copyright 479  
CoS 177  
country code 428  
creating certificates 306  
CTS (Clear to Send) 464  
custom ports  
creating/editing 254  
customer support 483  
customized services 254

Differential Binary Phase Shift Keyed Modulation 430  
Differential Quadrature Phase Shift Keying Modulation 430  
differentiated services 177  
Diffie-Hellman key groups 289  
DiffServ 177  
DiffServ code points 177  
DiffServ marking rule 177  
directory servers  
adding/editing 323  
certificates 302  
directory servers, and certificates 322  
disclaimer 479  
distinctive ring 202, 428  
DnD 428  
DNS 118, 352  
DNS Server  
for VPN host 280  
do not disturb 428  
domain name 375  
domain name system  
see DNS  
DoS 235  
basics 235  
types 236  
DoS attacks, types of 236  
DQPSK 430  
DS field 177  
DSCPs 177  
DSL line, reinitialize 421  
DSLAM (Digital Subscriber Line Access Multiplexer) 43  
DTMF 175  
DTMF detection and generation 429  
Dual-Tone MultiFrequency 175  
dynamic DNS 339  
dynamic jitter buffer 428  
dynamic secure gateway address 277  
dynamic WEP key exchange 469  
DYNDNS wildcard 339

## D

data confidentiality 270  
data integrity 270  
data origin authentication 270  
DBPSK 430  
default 412  
default LAN IP address 49  
Denial of Service 234, 235, 260  
destination address 247  
DH 289  
DHCP 118, 339, 375  
diagnostic 419

## E

EAP Authentication 467  
EAP-MD5 430  
echo cancellation 184, 429  
e-mail 148  
log example 391  
Emergency Numbers 184

emergency numbers **206**  
 encapsulated routing link protocol (ENET ENCAP) **101**  
 encapsulation **101, 271**  
   ENET ENCAP **101**  
   PPP over Ethernet **101**  
   PPPoA **102**  
   RFC 1483 **102**  
 encapsulation security payload **275**  
 encryption **269, 470**  
 ESP **271**  
 ESP protocol **275**  
 ESS **462**  
 Europe type call service mode **195**  
 Extended Service Set IDentification **134**  
 Extended Service Set, See ESS **462**  
 extended wireless security **74**  
 external antenna **429**  
 external RADIUS **430**

FTP **159, 348**  
   file upload **417**  
 FTP restrictions **408**

## G

G.168 **184, 429**  
 G.711 **429**  
 G.726 **429**  
 G.729 **429**  
 G.992.1 **426**  
 G.992.3 **426**  
 G.992.4 **426**  
 G.992.5 **426**  
 general setup **375**  
 Graphical User Interface (GUI) **42**  
 group ring **202, 428**

## F

F4/F5 OAM **426**  
 FCC interference statement **479**  
 filename conventions **407, 408**  
 firewall  
   access methods **245**  
   address type **253**  
   alerts **248**  
   anti-probing **259**  
   creating/editing rules **251**  
   custom ports **254**  
   enabling **248**  
   firewall vs. filters **243**  
   guidelines for enhancing security **242**  
   introduction **234**  
   LAN to WAN rules **248**  
   policies **245**  
   rule checklist **246**  
   rule logic **246**  
   rule security ramifications **246**  
   types **233**  
   when to use **243**  
 firmware **408**  
   upload **409**  
   upload error **410**  
 firmware upgrade **428**  
 flash key **195**  
 flashing **195**  
 fragmentation threshold **464**  
 frame relay **43**  
 frequency range **430**

half-open sessions **260**  
 hidden node **463**  
 host **376**  
 hot line **428**  
 HTTP **234, 235**  
 HTTP (Hypertext Transfer Protocol) **409**  
 HTTPS **345**  
   and remote management **345**  
   implementation **345**  
   introduction **345**  
 humidity **423**

## I

IANA **119, 460**  
   Internet Assigned Numbers Authority  
     see IANA  
 IANA (Internet Assigned Number Authority) **254**  
 IBSS **461**  
 ICMP echo **237**  
 ID type and content **281**  
 IEEE 802.11g **429, 430, 465**  
 IEEE 802.11g data rates **430**  
 IEEE 802.11g modulation **430**  
 IEEE 802.11g wireless LAN **429**

IEEE 802.11i **430**  
IEEE 802.1Q VLAN **177**  
IGMP **120**  
IGMP proxy **426**  
IGMP v1 **426**  
IGMP v2 **426**  
IKE phases **288**  
importing certificates **304**  
importing trusted CAs **313**  
importing trusted remote hosts **319**  
Independent Basic Service Set  
    See IBSS **461**  
initialization vector (IV) **470**  
inside header **272**  
install UPnP **363**  
    Windows Me **363**  
    Windows XP **364**  
Integrated Access Device **41**  
internal calls **227, 428**  
Internet access **63**  
internet access **43**  
Internet access wizard setup **63**  
Internet Assigned Numbers Authority  
    See IANA  
Internet Control Message Protocol (ICMP) **237**  
Internet Key Exchange **288**  
Internet Protocol Security **269**  
Internet Telephony Service Provider **43**  
IP address **118, 160, 161**  
IP address assignment **102**  
    ENET ENCAP **103**  
    PPPoA or PPPoE **103**  
    RFC 1483 **103**  
IP alias **425**  
IP multicasting **426**  
IP network and PSTN connection **211**  
IP Policy Routing (IPPR) **425**  
IP pool **125**  
IP pool setup **118**  
IP spoofing **236, 238**  
IP to IP Calls **44**  
IPSec **269**  
IPSec algorithms **271, 275**  
IPSec and NAT **272**  
IPSec architecture **270**  
IPSec passthrough **427**  
IPSec standard **425**  
IPSec VPN capability **425**  
ISDN (Integrated Services Digital Network) **42, 184**  
ITSP **43**  
ITU-T **184**

ITU-T G.992.1 **421**

## J

jitter buffer **428**

## K

keep alive **279**  
key fields for configuring rules **247**  
keys and certificates **301**

## L

LAN setup **101, 117**  
LAN TCP/IP **118**  
LAND **236, 237**  
LEDs **46**  
listening port **182**  
log out **52**  
log out (automatic) **52**  
login **50**  
logs **381, 387**

## M

MAC address filter action **144**  
MAC filter **143**  
Management Information Base (MIB) **350**  
managing the device  
    good habits **42**  
    using FTP. See FTP.  
    using Telnet. See command interface.  
    using the command interface. See command interface.  
Maximum Burst Size (MBS) **104, 109, 113**  
max-incomplete high **260**  
max-incomplete low **260**  
Message Integrity Check (MIC) **470**  
metric **103**  
multicast **120**  
multimedia **169**  
multiple PVC support **425**

multiple SIP accounts **429**  
 multiple voice channels **429**  
 multiplexing **102**  
   LLC-based **102**  
   VC-based **102**  
 multiprotocol encapsulation **102**  
 music on hold **428**  
 my IP address **276**

**N**

nailed-up connection **103**  
 NAT **119, 160, 460**  
   address mapping rule **164**  
   application **156**  
   definitions **155**  
   how it works **156**  
   mapping types **157**  
   what it does **156**  
 NAT (Network Address Translation) **155**  
 NAT mode **159**  
 NAT sessions **427**  
 NAT traversal **280, 361**  
 negotiation mode **289**  
 NetBIOS commands **238**  
 Network Address Translation  
   see NAT

**O**

OAM **426**  
 OFDM **431**  
 OK response **173, 175**  
 one-minute high **260**  
 Orthogonal Frequency Division Multiplexing  
   Modulation **431**  
 outside header **272**

**P**

packet filtering **243**  
   when to use **243**  
 packet filtering firewalls **233**  
 Pairwise Master Key (PMK) **470, 472**  
 park **427**  
 password

change at login **50**  
 password change at login **51**  
 Peak Cell Rate (PCR) **104, 109, 113**  
 peer call authentication, VoIP trunking **212**  
 peer IP **217**  
 peer port **217**  
 peer-to-peer calls **44**  
 Perfect Forward Secrecy **289**  
 per-hop behavior **177**  
 Permanent Virtual Circuits **426**  
 PFS **289**  
 PHB (Per-Hop Behavior) **177**  
 phone **183**  
 phone config **428**  
 pickup **427**  
 ping of death **236**  
 PKI (Public-Key Infrastructure) **302**  
 point to point calls **44**  
 Point to Point Protocol over ATM Adaptation Layer 5  
   (AAL5) **102**  
 point-to-point calls **429**  
 POP3 **235**  
 port forwarding **427**  
 power adaptor **431**  
 power specifications **423**  
 PPP (Point-to-Point Protocol) Link Layer Protocol **426**  
 PPP over ATM AAL5 **426**  
 PPP over Ethernet **426**  
 PPPoE **101**  
   benefits **101**  
 PPPoE (Point-to-Point Protocol over Ethernet) **101,**  
   **425**  
 preamble mode **465**  
 pre-shared key **283**  
 priorities **333**  
 priority **335**  
 private keys, and remote management **345**  
 product registration **481**  
 PSK **470**  
 PSTN call setup signaling **175**  
 public keys, and remote management **345**  
 Public Switched Telephone Network **41**  
 public-key cryptology, and certificates **301**  
 public-private keys  
   and certificates **301**  
 pulse dialing **175**  
 PVCs **426**

**Q**

QoS **176, 429**  
 Quality of Service **176, 429**  
 quick dialing **429**  
 Quick Start Guide **49**

**R**

RADIUS **430, 466**  
 message types **467**  
 messages **467**  
 shared secret key **467**  
 Reach-Extended ADSL **426**  
 Real time Transport Protocol **173**  
 real-time e-mail alerts **426**  
 recurity ramifications **246**  
 region **428**  
 registration  
   product **481**  
 reinitialize the ADSL line **421**  
 related documentation **3**  
 remote hosts, and certificates **316**  
 remote management  
   and certificates **345**  
   and HTTPS **345**  
   and private/public keys **345**  
   and SSL **345**  
   how SSH works **355**  
   HTTPS example **345**  
   secure FTP using SSH **358**  
   secure telnet using SSH **357**  
   SSH **354**  
   SSH implementation **356**  
 remote management and NAT **344**  
 remote management limitations **344**  
 REN **428**  
 reports and logs **426**  
 reset button **47**  
 resetting your device **47**  
 restore **411**  
 restore configuration **416**  
 RF (Radio Frequency) **431**  
 RFC 1483 **102, 426**  
 RFC 1631 **155**  
 RFC 1889 **173, 429**  
 RFC 1890 **429**  
 RFC 2327 **429**  
 RFC 2364 **426**  
 RFC 2516 **425, 426**

RFC 2684 **426**  
 RFC 3261 **429**  
 Ringer Equivalence Number **428**  
 ringing **428**  
 RIP **120**  
   direction **120**  
   Routing Information Protocol  
     see RIP  
   version **120**  
 romfile **407**  
 RTCP **429**  
 RTP **173, 429**  
 RTS (Request To Send) **464**  
   threshold **463, 464**  
 rules **248**  
   checklist **246**  
   key fields **247**  
   LAN to WAN **248**  
   logic **246**

**S**

SA **269**  
 safety warnings **6**  
 saving the state **238**  
 SDP **429**  
 seamless rate adaptation **426**  
 secure FTP using SSH **358**  
 secure gateway address **276**  
 Secure Socket Layer (SSL) **345**  
 secure Telnet using SSH **357**  
 security  
   and certificates **301**  
 security association **269**  
 security in general **242**  
 Security Parameter Index **292**  
 server **157, 158, 378**  
 service **247**  
 Service Set **134**  
 service type **255**  
 services **160**  
 Session Description Protocol **429**  
 Session Initiating Protocol **429**  
 Session Initiation Protocol **169**  
 silence suppression **184, 429**  
 Single User Account (SUA) **43**  
 SIP **169**  
 SIP account **169**  
 SIP accounts **429**

SIP ALG **429**  
 SIP ALG passthrough **426**  
 SIP Application Layer Gateway **429**  
 SIP authentication password **80**  
 SIP authentication user ID **80**  
 SIP call progression **173**  
 SIP client **170**  
 SIP identities **169**  
 SIP INVITE request **173, 174**  
 SIP number **80, 169**  
 SIP OK response **175**  
 SIP proxy server **170**  
 SIP redirect server **171**  
 SIP register server **172**  
 SIP server address **80**  
 SIP servers **170**  
 SIP service domain **80, 170**  
 SIP URI **169**  
 SIP user agent **170**  
 SIP version 2 **429**  
 SMTP error messages **390**  
 smurf **237**  
 SNMP **349, 426**  
   manager **350**  
   MIBs **350**  
 SOHO (Small Office/Home Office) **43**  
 source address **247**  
 speed dial **198, 227**  
 SPI **292**  
 SRA **426**  
 SSH **354**  
   how SSH works **355**  
   implementation **356**  
 SSL (Secure Socket Layer) **345**  
 stateful inspection **233, 234, 238, 239**  
   on your ZyXEL device **240**  
   process **239**  
 stateful packet inspection **426**  
 static route **327**  
 SUA **158**  
 SUA (Single User Account) **158**  
 SUA vs NAT **158**  
 subnet **453**  
 subnet mask **118, 253, 454**  
 subnetting **456**  
 supplementary services **194**  
 Sustain Cell Rate (SCR) **109, 113**  
 Sustained Cell Rate (SCR) **104**  
 SYN flood **236, 237**  
 SYN-ACK **236**  
 syntax conventions **4**

syslog **258**  
 system name **376**  
 system timeout **344**

## T

TCP maximum incomplete **260**  
 TCP security **240**  
 TCP/IP **235, 236**  
 teardrop **236**  
 Telnet **347**  
 temperature **423**  
 Temporal Key Integrity Protocol (TKIP) **470**  
 TFTP  
   file upload **417**  
 TFTP and FTP over WAN **408**  
 TFTP restrictions **408**  
 three-way conference **196, 197**  
 three-way handshake **236**  
 threshold values **259**  
 TLS **430**  
 ToS **177**  
 traceroute **238**  
 trademarks **479**  
 traffic redirect **114, 116**  
 traffic shaping **104**  
 transparent bridging **426**  
 transport mode **272**  
 trunking **428**  
 trunking, VoIP **211**  
 trusted CAs, and certificates **311**  
 TTLS **430**  
 tunnel mode **272**  
 Type of Service **177**

## U

UBR (Unspecified Bit Rate) **109, 113**  
 UDP/ICMP security **241**  
 Uniform Resource Identifier **169**  
 Universal Plug and Play **361**  
   application **361**  
 Universal Plug and Play (UPnP) **425**  
 upload firmware **416**  
 UPnP **361**  
   forum **362**  
   security issues **361**

upper layer protocols **240, 241**  
USA type call service mode **196**  
using speed dial **227**

## V

VAD **184, 429**  
VBR (Variable Bit Rate) **113**  
VBR-nRT **109**  
VBR-RT **109**  
Virtual Channel Identifier (VCI) **102**  
Virtual Circuit (VC) **102**  
Virtual Local Area Network **177**  
Virtual Path Identifier (VPI) **102**  
Virtual Private Network **269, 425**  
VLAN **177**  
VLAN group **177**  
VLAN ID **177**  
VLAN ID tags **177**  
voice activity detection **184, 429**  
voice channels **429**  
voice coding **175**  
VoIP **169**  
    ring selection **202**  
    testing rings **203, 205**  
VoIP links **211**  
VoIP standards compliance **429**  
VoIP trunking **211**  
    and security **211**  
    call rules **213**  
    detailed example **219, 220, 221, 222, 224**  
    examples **213, 214**  
    how it works **211**  
    overview **211**  
    peer authentication **216**  
    peer calls **215**  
    scenarios **213, 214**  
    SIP settings **214**  
    web configurator **214**  
VPI & VCI **102**  
VPN **269**  
VPN applications **270**

## W

WAN (Wide Area Network) **101**  
WAN to LAN rules **248**  
warranty **481**

note **481**  
Web **346**  
Web Configurator **49, 241, 242, 247**  
    and VoIP trunking **214**  
WEP (Wired Equivalent Privacy) **430**  
WEP encryption **137, 152, 153**  
Wi-Fi Protected Access **469**  
Wi-Fi Protected Access (WPA) **430**  
wireless client WPA supplicants **471**  
wireless LAN MAC address filtering **429**  
wireless security **465**  
WLAN  
    interference **463**  
    security parameters **472**  
WPA **469**  
    key caching **470**  
    pre-authentication **470**  
    user authentication **470**  
    vs WPA-PSK **470**  
    wireless client supplicant **471**  
    with RADIUS application example **471**  
WPA2 **469**  
    user authentication **470**  
    vs WPA2-PSK **470**  
    wireless client supplicant **471**  
    with RADIUS application example **471**  
WPA2-Pre-Shared Key **469**  
WPA2-PSK **469, 470**  
    application example **471**  
WPA-PSK **469, 470**  
    application example **471**  
WWW **148**

## Z

zero configuration Internet access **105, 425**  
ZyNOS **408**  
ZyNOS (ZyXEL Network Operating System) **408**  
ZyNOS F/W version **408**  
ZyXEL's firewall  
    introduction **234**